AN EXAMINATION OF EXISTING FEDERAL STATUTES ADDRESSING INFORMATION PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON
COMMERCE, TRADE AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

APRIL 3, 2001

Serial No. 107–22

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE
71–499PS WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN MCCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

NATHAN DEAL, Georgia
Vice Chairman
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ED BRYANT, Tennessee
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
GREG WALDEN, Oregon
LEE TERRY, Nebraska
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

EDOLPHUS TOWNS, New York
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

AN EXAMINATION OF EXISTING FEDERAL STATUTES ADDRESSING INFORMATION PRIVACY

TUESDAY, APRIL 3, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2 p.m., in room 2123 Rayburn House Office Building, Hon. Cliff Stearns (chairman) presiding.

Members present: Representatives Stearns, Deal, Shimkus, Buyer, Pitts, Terry, Tauzin (ex officio), Towns, DeGette, Markey, and Gordon.

Staff present: Ramsen Betfarhad, professional staff; Mike O'Rielly, professional staff; Kelly Zerzan, majority counsel; Anthony Habib, legislative clerk; and Bruce Gwinn, minority counsel.

Mr. STEARNS. The subcommittee will come to order. Good afternoon, everybody. Welcome to the Subcommittee on Commerce, Trade and Consumer Protections, third in a series of hearings on information privacy. I thank the witnesses for appearing before the subcommittee today. I especially want to thank members for attending a Tuesday afternoon hearing. I know that at times it's difficult for many members to be back from their home districts in time for a Tuesday afternoon hearing.

Our witnesses today will explain and examine a number of Federal statutes addressing personal information privacy. Their collective testimonies present a mere snapshot of the array of the existing Federal statutes speaking to the issue of information privacy.

I understand that there are over 30 Federal statutes alone. Moreover, there are hundreds of State statutes dealing with information privacy in some form or another. Those Federal and State statutes have a wide range, both in their scope and depth of coverage. They implicate personal information used across many sectors of the economy and for differing commercial activities, while offering varied levels of protection depending on the type and use of the personal information.

Among the 30-odd Federal statutes are ones addressing the disclosure of sensitive personal financial information used for substantive purposes such as credit and employment decisions. There are such statutes protecting children's personal information on line, students' information, certain personal data garnered by commu-

nications providers, date stored on-line, medical information privacy and so on.

As for the State statutes, they tend to govern the personal information, the rich world of public records. For example, the collection and use of personal information relating to real estate transaction or divorce proceedings are all governed by State statutes.

The disclosure and use of information required by licenses such as those for business, hunting, fishing, professional practices such as medicine, are all governed by State statute. The universe of both Federal and State statutes speaking to information privacy is instructive for three important reasons. First, the existence of those statutes suggest that concerns over information privacy are not new.

Second, the statutes tell us that both the Congress and statute legislatures have acted to protect the privacy of certain types of personally identifiable information upon finding a harm. And finally, the review of existing statutes permits the subcommittee to hone in on areas where there is no existing legal regime protecting information.

Upon identification of the implicated area, or type of information and its usage not protected by law, the subcommittee's inquiry will shift to investigating whether consumers are harmed by the lack of such legal protections. If harm is found, then any legal fix contemplated must meet a cost and benefit analysis. That is to say, that the extent of the identified harm must be measured against the benefits accruing to our economy from the free flow of the implicated type information.

The testimony today clearly shows that the information privacy debate is rich in history and has evolved throughout many years. In the subcommittee's first information privacy hearing we learned that the first amendment sets the outer limits of our information privacy inquiry today as the first amendment sets the outer parameters of the debate.

The existing Federal and State statutes addressing information privacy narrow our inquiry and debate even further. On a different note, I wish to commend the Administration for taking a more proactive approach in dealing with the ramifications for American businesses of the European Commission's data protection directive. The joint letter by the Treasury and Commerce Departments to Mr. John Mogg of the European Union Commission dated March 23 regarding "model contracts" is important because it signals the Administration's interest in and concern over this matter.

The subcommittee in its March 8 hearing was the first congressional forum to focus on the ramifications of the EU data protection directive for international commerce and just as I said at that hearing, I am very concerned about the potentially regressive impact of the directive and its implementing statutes. I'm pleased that the Administration has begun to engage the issue.

This subcommittee will continue its examination of not only the data protection directive, but also other nuances, legal or regulatory impediments on international commerce and especially dealing with E-commerce.

And I'm pleased to recognize the ranking member, the gentleman from New York, Mr. Towns.

Mr. TOWNS. Thank you very much, Mr. Chairman. I would also like to thank all of the witnesses. I look forward to your testimony.

When this subcommittee was charged with discussing the issue of privacy, I made it a priority to meet with many of the New York Silicon Alley companies and consumers to hear diverse views on this topic. And while many had different views on how privacy should be protected and what was necessary to protect it, each side agreed that every company doing business in the on-line and off-line world should have a public/private policy that is written in plain English and adhered to once the policy is made public.

When a company such as TiVo acts in bad faith and breaks their own privacy policy, misleading its customers, the FTC and the courts should hold them accountable. While bad actors have always been burdensome to legitimate business, I am heartened by new technologies that are being developed so that the public will have more control over when and to whom they dispense their valuable personal information.

Microsoft's platform for privacy protection or P3P and Hailstorm and dot net technology will allow consumers to see a particular website's privacy policy in a clear, effective manner and allow them to set privacy limits which will provide consumers with clear information as to the privacy practices of an on-line company, giving individuals more control over their personally identifiable information.

Location privacy is another concern of my constituents as well. The wireless industry has been aware of the public's concern and worked with members of the committee to enact CPNI standards. They also voluntarily with principles such as notice consent, security and integrity. These are just two examples of industry understanding their privacy and the protection of privacy can be positive not only for the consumer, but for their bottom line as well.

Another concern of my constituents is making sure that we protect kids both on-line and off-line from predatory business practices. Many have spoken to me about COPPA and complain about how government quickly passed a law without consulting businesses, simply tossing aside the notion of self-regulation. I plainly point out to my friends that on two separate occasions the previous Administration asked industry to clean itself up and protect children and much to my chagrin the majority of the industry took little or no notice of that fact.

I want to avoid drowning in the wash of misguided privacy legislation in this Congress. Let's listen to all sides of the debate and if we can agree on a sensible legislation, let's make sure we get it right the first time, rather than have to do it over a month or a year from now because we did not do it right the first time.

Mr. Chairman, on that note, I will yield back the balance of my time.

Mr. STEARNS. The gentleman yields back. Thank you. The ranking member, Mr. Deal of Georgia is recognized for an opening statement.

Mr. DEAL. I have no statement.

Mr. STEARNS. Ms. DeGette?

Ms. DEGETTE. Thank you, Mr. Chairman. I'd like to thank you for holding another, in a series of privacy hearings that we've un-

dertaken in the subcommittee and right out of the gate too. The Privacy Foundation, who we'll hear from today is based out of Colorado and has been working with the University of Denver Privacy Center on the Report on TiVo, Inc. that will be referred to in the hearing. I want to thank the Foundation for its good work and especially welcome Mr. Smith who is sitting here, our witness, the Chief Technology Officer of the Privacy Foundation, who unfortunately is not my constituent, I understand is from all of our good friend, Ed Markey's home district.

An examination of existing Federal statutes should prove to be quite informative, although I think it's a rather large task to undertake in one hearing. I think that we probably could have benefited from having witnesses from the Federal agencies responsible for carrying out some of these congressionally mandated statutes and I hope we'll be able to include such witnesses at related hearings in the future.

The issue of privacy gets more timely every day. I'm sure, Mr. Chairman, you and my other colleagues saw the article in the Washington Post this morning reporting on the new Pew Foundation Report entitled "Fear of On-Line Crime" which addresses Americans' views on the need for on-line privacy protection.

This report gives some very interesting insights into how the American consumer feels about privacy. On the one hand, a large percentage of people think that action definitely needs to be taken to protect their personal information from being exploited on-line. By the same token, it appears as if they do not really trust the government, business or anyone else to do the right thing on this issue.

I gave a speech this morning, for example, to the American Teleservices Association and got to hear their concerns with privacy, both from a business standpoint regarding their fears that legislation could undermine the competitiveness of their companies and also their fears about State legislation and creating a patchwork of oftentimes competing statutes. But also, they were concerned as individuals about their personal information getting out. And so the one thing that has really struck me recently is how truly conflicted people are about the issue of privacy and that's convinced me even further that we as Federal legislators needs to be very careful. I'd like to echo my colleague Mr. Towns. We need to be very careful as we proceed down this road toward privacy regulation. We need to make sure we know what we are doing, not always readily apparent with Congress, and when we act we need to do it right the first time.

I'm looking forward to hearing the testimony of the witnesses, Mr. Chairman, and yield back the balance of my time.

Mr. STEARNS. The gentle lady yields back the balance of her time and I would indicate to her that we intend to have a hearing on the Pew Internet and American Life Project Survey as well as others at a future date and I appreciate bringing that to the committee's attention.

Now I recognize the distinguished chairman of the full committee, Mr. Tauzin of Louisiana.

Mr. TAUZIN. Thank you, Mr. Chairman, and let me thank you for conducting this series of hearings. This is the third hearing on pri-

vacy already this year. And the thoughtful approach is, I think, absolutely called for here. Obviously, looking back and seeing what we have done in privacy, how it has worked, what is left to be done are critical elements of these hearings. And I think those are the three themes, I think, we ought to think about today.

What have we done in critical areas and what is left to be done and what have we done wrong? What's really not working well, before we go forward with new proposals to enact new privacy legislation. We're going to get enlightened today and I'm particularly pleased to hear from folks like those at AT&T who are going to give us a look at how corporate America can tell a good story about how they are protecting the privacy of citizens and perhaps a story that isn't often focused on when we hear the horror stories about how privacy sometimes gets violated.

We know, for example, that corporate America is learning very quickly good privacy protection is good for business, that consumers who focus on security and privacy of their information do tend to gravitate toward companies that respect the privacy of that information and provide security for that information where privacy needs protection.

It's important also to note that the issue of privacy is not new to this committee or to Congress, in general. It's not something we just dreamed up this year or the last five or 10 years because of the Internet. U.S. privacy laws have literally developed pretty much in the piecemeal basis, as we saw the need, as we saw a problem. A good example is the Video Privacy Act.

You recall the efforts to review a Supreme Court nominee's video rentals and how this offended not just that nominee, but I think the American public, in general, that anyone should be making public the video rentals of a citizen of a country just to expose some dirt that might disable their career.

I frankly think that approaching privacy on this piecemeal basis has had some merit. We can, for example, learn that privacy means something different in different areas of our human activities. We also learn, Mr. Chairman, I want to thank you for that great hearing on the EU comprehensive regime. We learned how a comprehensive approach can sometimes present real problems when it comes to specific elements of commercial and human activity. And on that note, let me comment on the dispute regarding the EU data privacy directive that was the subject of your last hearing. We're very pleased to see that the new Administration's letter to our European colleagues questioning the so-called model contracts and seeking additional discussions on the matter.

This subcommittee, in fact, highlighted the need for the Administration to be on top of that issue and it looks like you got their attention, Cliff. I'm very pleased for that. As presented to us, it seems that the model contracts are an effort to undercut the so-called safe harbor and further impose a European privacy approach on the United States and I think it's clear that Europeans do not understand U.S. business practices, behaviors or policies or even our customers and they seem also to be unaware of the vast benefits of informational exchanges.

I see, I think, now the Administration sees the need for negotiations on this issue in the near future, as this will have a larger and larger impact on our trade relations with the Europeans.

I want to also compliment the Administration on their attention and their additional involvement to find indeed an acceptable outcome for all the parties.

Last, I hope we get a chance at this hearing or future ones, to touch upon the real and potential unintended consequences in current statutes. For example, while everyone agrees that protecting the privacy of children as they navigate the Internet, evidence now suggests that the existing statute, the Child On-Line Privacy Protection Act, COPPA, has now forced companies to discontinue a number of products targeted toward children. Instead of complying with the statute, a number of sites just stopped serving users who are less than 13 years of age and while this sounds positive, there's some downsides to it that we ought to be concerned about.

If we end up forcing private companies and nonprofits to eliminate beneficial products such as crime prevention material, have we done a good thing? If teen-friendly sites, those that totally respect the privacy of the users stop offering e-mail services to children, is that a good thing? And if kids end up lying about their age just to qualify for certain features, is that a good thing?

I suppose, Mr. Chairman, what I'm saying is we can learn a lot from the experience of the privacy statutes that we've already passed and the more we learn about those statutes, the more thoughtfully and carefully we can navigate what remains to be done. The universe of areas where citizens still are urging us to legislate.

Mr. Chairman, this is a good line up as I know your future hearings will be and as I am certain your past hearings have been.

Thank you for this one and I yield back the balance of my time.

Mr. STEARNS. And I think the chairman. I think your statement, learning from privacy statutes that already have passed is extremely important and we're delighted to do that.

The gentleman from Tennessee, Mr. Gordon, is recognized.

Mr. GORDON. I'll make my statement a part of the record and I'm ready to move to the witnesses.

Mr. STEARNS. All right, the gentleman yields back. Mr. Terry?

Mr. TERRY. Same.

Mr. STEARNS. Same, okay.

Mr. Pitts?

Mr. PITTS. Thank you, Mr. Chairman, I'll submit my opening statement for the record.

Mr. STEARNS. Okay, Mr. Buyer?

Mr. BUYER. Add me in.

Mr. STEARNS. Okay. I'm delighted to welcome the first panel and as our distinguished chairman has talked about, it's not often that you have a hearing in Congress where you actually look at existing statutes that have already passed and people might say well, this might be a dry hearing and that possibly be true, but before you're going ahead to pass new statutes, it's fundamental, I think, in Congress to go and look at what's existing. I'm delighted to have Michael Lamb, Chief Privacy Officer for AT&T Corporation; Ms. Anne Fortney, Managing Partner, Lovells; Mr. Rick Fischer, Partner,

Morrison and Foerster; and Mr. Richard Smith, Chief Technology Officer, The Privacy Foundation.

So welcome and we'd like to have each of you provide your opening statement and I would—hopefully, you can stay within 5 minutes.

Mr. Lamb?

STATEMENTS OF MICHAEL C. LAMB, CHIEF PRIVACY OFFICER, AT&T CORPORATION; ANNE P. FORTNEY, MANAGING PARTNER, LOVELLS; L. RICHARD FISCHER, PARTNER, MORRISON AND FOERSTER; AND RICHARD M. SMITH, CHIEF TECHNOLOGY OFFICER, THE PRIVACY FOUNDATION

Mr. LAMB. Thank you, Mr. Chairman and members of the committee for this opportunity. I applaud the committee's examination of the privacy issues in industry and that our consumers face under the existing statutes. It's a complex area and it affects every business and every consumer that we serve and we take it seriously, but it deserves the thorough and thoughtful process that I see underway here.

I've been asked to discuss, in particular, the Federal statutes that apply to AT&T's scope of activities which makes sense, in particular, telephony, wireless services, our array of broadband services, both cable programming and broadband telephony and broadband data as well as the Internet and on-line services. And in particular, I want to touch on four Federal statutes. By definition, it will be a whirlwind tour to discuss four fairly detailed statutes in this time. So I just want to touch on highlights and how these statutes overlap and how they treat privacy slightly differently.

Each statute was enacted with the right goal, preserve privacy, help consumers' expectations be met with respect to privacy. They all took a somewhat different approach. In industry, we work within this framework, but sometimes we find that two or three different, and indeed conflicting, statutes will sometimes apply to a single service and that makes our lives difficult.

I'm going to discuss the Customer Proprietary Network Information or CPNI rules in the Communications Act. They apply to telephony services. The Cable Act privacy provisions, the Electronic Communications Privacy Act or ECPA which deals in particular with privacy of e-mail and voice mail and advanced electronic communications. And then finally, I'll touch on the Telephone Consumer Protection Act which is really a consumer choice statute that goes across industry and deals with telephone solicitations and how companies can use the data or not use it in their telephone solicitations.

And I think you'll see differences in approaches and some overlaps in these statutes that we live with today. There's room for refinement, but it is a system that works and I think we can all learn from what's been done.

The CPNI rules in Section 222 of the Communications Act apply to telecommunications services offered by a carrier. And it's a very detailed privacy statute that in turn gave authority to an agency to enact even more detailed rules. That gives us some degree of certainty about the nature of the obligation, but it also leads to com-

plications as we apply these in our data bases and customer bills and the like.

In a nutshell, the CPNI rules define certain information such as whom customers call and their location and how much they spend as data that will be subject to extra privacy protections and then define certain other data including name, address and telephone number and aggregated information as not being CPNI, where the companies are free to use that information subject to their own public/privacy policies.

Without customer approval, a carrier may only use CPNI for the service category from which they obtained it. Therefore, AT&T, for example, can only use our long distance data as we market and provide long distance services and could not use that even internally to offer local exchange service, for example.

So this is both an internal restriction and a restriction on our disclosure to third parties.

The CPNI Act contains no disclosure obligations and no restrictions on collecting information. You'll see in that respect it varies somewhat from some of the other statutes.

Now our discussion gets a little more interesting when we look at the interplay between the CPNI rules and the next section I wanted to discuss which is Section 631 of the Cable Act. Section 631 applies to all cable services and other services offered over cable facilities and instantly from that definition we can see that when one turns to telephone service offered over a cable facility, you're under two different statutory frameworks. And indeed, we'll see that when you look at data services, you also are under multiple frameworks. In some ways we can comply with both sets. You'll see a couple of conflicts where we have difficulty resolving the differences in approach.

Section 631 has a notice obligation. As a cable operator, AT&T sends an annual, written privacy notice that describes our practices to each of our cable customers and both how we use it internally and what data we collect. It also somewhat more flexibility on a company's internal use of data which is consistent with what we've seen consumer concerns. Consumers sometimes are much more concerned about disclosing to third parties than they are the use of data within a single company with whom they know they're doing business.

One particular problem arises under the Cable Act in the law enforcement sections. Under the Cable Act, a company like AT&T can only disclose personally identifiable data concerning our cable customers to law enforcement if there's a court order which we have no issues with, but also if we have given prior notice to our customers.

And where we run into difficulties is when law enforcement requests data and provides a court order and asserts that notifying a customer could compromise an on-going law enforcement investigation and there is no exception in the statute and that leads me to my third statute which is ECPA which arguably governs data services such as e-mail and the like provided over a cable system. And ECPA also has detailed rules on when we provide data to law enforcement and it says that typically for e-mail contents, for example, prior notice must be given unless law enforcement tells us

that such notice would endanger an on-going investigation or compromise it.

So law enforcement agencies will come to AT&T with an appropriate court order and claim that ECPA applies to an e-mail that was sent over a cable system and then we're faced actually with a devil's choice between two conflicting statutes and our approach has been to let the courts decide. If a court orders us to turn over data and a court orders us not to disclose that to our customer, then we have to comply with the lawful court order. But there indeed is a conflict between the two statutes on that point.

We also see under ECPA——

Mr. STEARNS. I just want you to sum up, if you can. I know how difficult considering the complexity of it.

Mr. LAMB. Absolutely. The last statute I want to turn to is the TCPA which basically allows customers or other individuals to be put on a do not call list for companies and that really is a choice statute. It applies across industries. It says you may have information about me, but I don't want you to call me using that information. And it boils down to that basic approach, the statute has worked.

But also see unintended consequences even in that statute when a customer requests to be put on a do not call list, the telephone number is put on a list and it applies for 10 years. However, customers move. Some 15 to 20 percent of telephone numbers change every year, so we find that after 3 or 4 years, the vast, vast majority of the phone numbers on our list are completely out of date and no longer belong to the people who made the request. And just to sum up, I just want to say that responsible companies such as AT&T realize that privacy commitments are important to our customers and they're important to us. They are good business. We are under three or four or indeed a myriad of privacy regimes in the industries in which AT&T operates, but all of our customers receive a high standard of privacy and that is because of the self-regulation efforts that we partake in with our own voluntary privacy policy as supplemented by the statutes and you can't look at any one set in isolation.

Thank you.

[The prepared statement of Michael C. Lamb follows:]

PREPARED STATEMENT OF MICHAEL C. LAMB, CHIEF PRIVACY OFFICER, AT&T CORP.

Thank you, Mr. Chairman. I am Michael Lamb, Chief Privacy Officer of AT&T Corporation. I applaud this Committee's examination of existing federal statutes that govern information privacy in various industry sectors.

I. INTRODUCTION AND SUMMARY

The Committee has asked me to discuss certain existing Federal statutes on information privacy that apply to AT&T's principal businesses. Today, my goal is to describe these statutes, and to point out some differences and overlaps in their terms. These statutes complement a regimen of self-regulation and voluntary privacy commitments by AT&T and other privacy leaders. For example, AT&T participates in the self-regulatory efforts of the Direct Marketing Association and BBBOnline, which supplement and strengthen the statutory privacy obligations. As a result, despite the different sets of statutory privacy requirements, AT&T's different categories of customers all enjoy very high standards of privacy protection.

Given AT&T's scope of activities, we may be unique in the degree to which different sets of federal statutory privacy rules apply to key aspects of our operations. AT&T serves both consumers and businesses of all sizes; our business includes tra-

ditional telephony services, wireless communications, broadband cable services, and a wide array of Internet and online services. My testimony provides a brief overview of the privacy provisions of the following four federal statutes that apply to parts of AT&T's operations:

- Communications Act provisions regarding Customer Proprietary Network Information;
- Cable Communications Policy Act;
- Telephone Consumer Protection Act; and the
- Electronic Communications Privacy Act.

The privacy provisions in each of these federal statutes were designed to increase the protection for information that companies may possess about customers and other consumers. There are both similarities and differences among these four statutes, however. The TCPA is narrowly focused and designed principally to restrict communications between firms and consumers—restrictions on telemarketing, for example. Other statutes, such as ECPA, are designed principally to protect information from interception by or disclosure to unauthorized third parties, including law enforcement agencies. The CPNI rules serve to restrict the use of customer information by telephone companies, both internally and vis-à-vis disclosure to third parties. And the Cable Act mandates detailed annual privacy disclosures to customers and imposes restrictions on disclosures to third parties but provides flexibility for a cable operator to use information internally.

II. THE COMMUNICATIONS ACT CPNI RULES

Section 222 of the Communications Act requires telecommunications carriers to protect the confidentiality of customer proprietary network information ("CPNI"), such as the telephone numbers called by customers and the length of time of the calls. Section 222 is an example of a detailed privacy statute which gave authority to the Federal Communications Commission ("FCC") to enact even more detailed privacy rules.

Section 222 defines "CPNI" as information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. The Act excludes from the definition of CPNI several categories of information, including:

- subscriber list information such as name, address and telephone number;
- aggregate customer information from which individual customer identities have been removed; and
- data from other sources such as data from non-telecom services and data purchased from third parties.

Section 222 provides that, except with customer approval, a carrier receiving or developing CPNI by virtue of providing a telecommunications service shall use individually identifiable CPNI only to provide the type of service from which the CPNI is derived. In applying this rule, the FCC divided telecom services into three categories: local; long distance and wireless services. Under the FCC approach, long distance CPNI can be used to provide and market long distance services, but generally may not be used to market local or wireless service, for example. The FCC also ruled that when a customer purchased service in more than one category from a carrier, the CPNI rules did not prevent the carrier from dealing with the customer on the basis of the overall service relationship, even though that relationship covered multiple service categories.

The FCC decided that customer consent for the purpose of Section 222 should mean express affirmative opt-in consent given after the customer has received notice of what the customer's CPNI rights were. These consent rules, together with the FCC's other implementing rules, were vacated on appeal by the Court of Appeals. See U.S. West, Inc. v FCC, 182 F3d 1224 (10th Cir. 1999). The Court held that the FCC's requirement of an affirmative opt-in consent violated the First Amendment by restricting protected commercial speech. The FCC has not yet acted on remand from the Court, although it believes that its rules, with the exception of the affirmative opt-in consent requirement, are still in effect.

Having restricted how information may be used by a carrier, Section 222 contains no further obligation on carriers to inform customers about how information is used and contains no restrictions on the collection of CPNI, just on its use and disclosure. There is no private right of action against carriers for violations of Section 222 and no express preemption of state laws.

III. THE CABLE ACT

As is true in the telecommunications industry, the historical commitment to consumer privacy in the cable industry is very strong. That historical commitment is bolstered by detailed privacy rules in Section 631 of the Cable Communications Policy Act of 1984, as amended by the Cable Television Consumer Protection and Competition Act of 1992 (47 U.S.C. 551, et seq.). Section 631 applies to cable services and to "other services" provided by the cable operator over cable facilities. Such "other services" arguably include not only traditional cable services but also broadband Internet service, telephony service and interactive television when these services are provided over cable facilities. As new services are provided via cable facilities, there may be some decisions about which privacy regime should apply. For example, Internet/online services offered over cable facilities are arguably subject to detailed strict Cable Act privacy rules that do not apply to other types of online services delivered via other media.

Section 631 requires cable operators to give each subscriber an annual notice concerning the personally identifiable information ("PII") that the operator collects. The notice must also describe how the subscribers' PII will be used and disclosed. Upon request by a subscriber, a cable operator also must give access to all PII about the subscriber that the cable operator collects and maintains.

The Cable Act generally prohibits the collection or disclosure of subscribers' PII without their prior written or electronic consent. There are, however, broad exceptions to this prior consent obligation. The exceptions include:

- the disclosure of customer names and addresses if customer notice and an opt-out opportunity is first provided and disclosure does not reveal viewing patterns or the nature of transactions performed by the customer; and
- disclosures that are "necessary to render, or conduct a legitimate business activity related to a cable service or other service provided by a cable operator."

Under the Cable Act, PII may only be disclosed to law enforcement officials pursuant to a court order. Moreover, the Act requires that such an order should only issue if the subscriber has been afforded an opportunity to appear and contest the law enforcement request for information.

A cable operator that violates the privacy protections set forth in Section 631 is subject to actual and punitive damages and to awards of attorneys' fees to prevailing plaintiffs. The statute defines "actual" damages to include liquidated damages computed at the higher of $100 a day for each day of violation or $1,000, whichever is higher. Thus, no actual harm arguably needs to be demonstrated to collect such "actual damages."

The broad scope of Section 631 creates certain tensions. Telephony service provided over telephone facilities is subject only to the CPNI rules set forth in Section 222 of the Communications Act. Telephony service provided by a cable operator over cable facilities appears also to be subject to Section 631, an entirely different set of rules. Although the details of CPNI implementation are currently unclear, the now-vacated rules issued by the FCC had different consent mechanisms, different notice procedures and different use restrictions than those in Section 631.

IV. ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communication Privacy Act of 1986 ("ECPA"), 18 U.S.C. 2510-2522; 2701; was enacted to address potential privacy issues related to the growing use of computers and other new forms of electronic communications. It added provisions to the federal criminal code that extended the prohibition against the unauthorized interception of communications to specific types of electronic communications, including e-mail, pagers, cellular telephones, voice mail, remote computing services, private communication carriers, and computer transmissions. The Act also identified situations and types of transmissions that would not be protected, most notably an employer's monitoring of employee electronic mail on the employer's system.

ECPA extended Title III privacy protections to the transmission and storage of e-mail and other digitized textual information. ECPA restricted government access to subscriber and customer records belonging to electronic service providers. Unless they have the consent of the subscriber or customer, government agencies must first secure a criminal warrant, court order, or an authorized administrative or grand jury subpoena to access service provider records.

ECPA requires the government to give a subscriber or user fourteen days' notice before information is disclosed, but it allows delayed notice if there are exigent circumstances such as cases in which notice may: endanger the life or physical safety of an individual; lead to flight from prosecution or destruction or tampering with evidence; or otherwise seriously jeopardize an investigation. 18 U.S.C. sec.

2705(a)(2). ECPA also states that a service provider has a defense to an ECPA violation if it provides information in good faith in response to a request by an investigative or law enforcement officer in emergency situations such as immediate danger of death or serious bodily injury to any person.

Thus, law enforcement agencies have the ability to obtain subscriber information under ECPA with an appropriate court order without notifying a subscriber in advance. In contrast to ECPA, the Cable Act has no provisions that allow information to be provided to law enforcement without notice to a subscriber if such notice would threaten an investigation or that address emergency situations.

This statutory approach creates an issue when law enforcement agencies seek the contents of e-mails from broadband Internet service providers who offer their services over cable facilities—the Cable Act mandates that the subscriber be notified before information is disclosed to an agency and ECPA contemplates only that the agency obtain a court order.

While ECPA was designed to protect the content of electronic communications, it revised the definition of content to specifically exclude the existence of the communication itself, as well as the identity of the parties involved. This means that government entities such as the Department of Justice and other law enforcement entities have a greater ability to obtain information about a subscriber's identity and about whether or not the subscriber sent or received a particular e-mail than the agencies have to obtain the contents of an e-mail itself.

Oddly, under ECPA, private parties have greater rights to obtain the contents of e-mails than law enforcement agencies. The Act requires law enforcement agencies to obtain a criminal warrant or court order whereas a private party in civil litigation can obtain such information simply by having a clerk issue a subpoena. Companies with a commitment to privacy, such as AT&T, address this situation by voluntarily committing to notify customers in advance of releasing personally identifiable information in response to a civil subpoena.

V. TELEPHONE CONSUMER PROTECTION ACT

The Telephone Consumer Protection Act of 1991 (47 U.S.C. 227) ("TCPA") was created to govern telephone solicitations and give the Federal Communications Commission rulemaking authority to prescribe regulations necessary to protect residential individuals' privacy by avoiding telephone solicitations to which they object. TCPA in essence is a consumer choice statute. It allows consumers to tell companies: you may have some personal information about me, but I have the right to restrict how you use it, at least with respect to telemarketing.

The Act, together with the FCC's implementing rules, require companies to maintain do not call lists of all individuals who have requested to be put on such lists. Unless a specific request is made, the individual's do not call request applies to the particular business making the call and not to affiliated entities. Under the FCC's rules, the do-not-call list obligations apply to the specifically-identified telephone numbers of the requesting individuals and thus do not continue to apply to all telephone numbers associated with a person's name. The do not call obligation lasts for ten years after a request is made.

The TCPA also prohibits telemarketing solicitations to consumers before 8 a.m. or after 9 p.m., local time. In addition, it bans unsolicited fax messages.

A person who has received more than one telephone call from a given company within any twelve-month period after making a do not call request may sue for a TCPA violation. The person may recover the greater of actual damages or $500.

A company must not only establish a do not call list, but also establish a do not call policy and make that policy available on demand. It also must train telephone solicitation personnel in the existence and use of the do not call list. A company has an affirmative defense to a TCPA violation if it can show that it established and implemented, with due care, reasonable practices and procedures to effectively prevent telephone solicitations in violation of the TCPA rules.

The do not call rules have worked fairly well. The ability to rely on the affirmative defense of having reasonable TCPA compliance procedures in effect is very important for a large company such as AT&T. If a complaining individual is on AT&T's do not call list and we believe that we did not call the person, it nevertheless is hard to prove a negative when a consumer claims that we DID place a call.

The ten year prohibition in the Act is an example of a provision that may warrant re-examination in light changed circumstances, such as of the pace with which people move and change telephone numbers in today's world. Do not call lists are based on telephone numbers. If 20% of the individuals on a do not call list move and get new numbers each year, the list will be almost entirely outdated well before the ten-year restriction expires.

VI. CONCLUSION

AT&T operates under a number of different, and sometimes conflicting, federal statutes governing information privacy. These statutes restrict AT&T's actions in some respects and impose costs on AT&T for customer notices and other requirements. Each one of these statutes was enacted to bolster the privacy protections for individuals, a goal that AT&T whole-heartedly shares. AT&T has a strong corporate commitment to privacy, founded on our view that respecting the concerns and interests of our customers is not only the right thing to do, but it also makes good business sense. In addition, we take seriously our various statutory privacy obligations. We understand that consumers want to know how private information about them will be used and we recognize that in the competitive marketplace we can only keep our customers happy by using such private information with integrity.

Indeed, AT&T's substantive privacy commitments for the services covered by these statutes, and for AT&T's other services, exceed the obligations set forth in these privacy statutes.

Again, I thank the Committee for the opportunity to participate in this hearing. I believe it is particularly important to understand the scope and overlaps of existing federal statutes before addressing potential changes in privacy rules. This hearing provides a valuable opportunity to discuss the practical consequences of the existing federal privacy statutes as part of a considered and thoughtful evaluation of privacy issues. AT&T looks forward to continuing to work with the Committee in its review of privacy issues.

Mr. STEARNS. Thank you, Mr. Lamb.

Ms. Fortney, you're recognized for 5 minutes.

STATEMENT OF ANNE P. FORTNEY

Ms. FORTNEY. Thank you, Mr. Chairman. Members of the subcommittee, I am Anne Fortney. I'm a partner in the Washington, DC office of the Lovells law firm. I appreciate the opportunity to be here today to talk about information——

Mr. STEARNS. Ms. Fortney, I'm just going to ask you to take the microphone just move it a little to your right.

Ms. FORTNEY. Can you hear me now?

Mr. STEARNS. Yes, that's much better.

Ms. FORTNEY. Thank you. Thank you for telling me that. Thank you also again for allowing me to participate into today's hearing.

My testimony discusses the Fair Credit Reporting Act. I have more than 25 years' experience working with the Fair Credit Reporting Act and other consumer financial services' laws. This experience includes enforcing the Fair Credit Reporting Act while serving as Associate Director for Credit Practices at the Federal Trade Commission and interpreting the Act while working as in-house counsel for a national retail creditor. More recently in the private practice of law, I have helped clients in the consumer reporting and credit granting industries comply with this complex law. Based on this experience I can say that the Fair Credit Reporting Act is a remarkable statute, but it is also a unique statute carefully tailored to a unique industry.

There are several ways in which the consumer reporting industry is unique. The first is the significance of a consumer report information to this industry. While other businesses may collect and disclose consumers' confidential information obtained in the course of their dealings with consumers, in the course of the consumer reporting industry, this confidential information is the stock and trade of the companies involved. Consumer reporting agencies collect the information for the purpose of selling it to creditors, employers and others with legitimate uses for the information. This

fact is significant in terms of the industry's desire that the information be as accurate and complete as possible.

In addition, consumer report information is usually housed in central repositories. This fact is germane to the relative ease with which consumer reporting agencies may give consumers access to records held concerning them. And this is in contrast to other businesses which may not have other information compiled in such a central location. The fact that consumer reporting agencies house this information in a central data base is also relevant in terms of the ability of these companies to successfully limit disclosure to those having a permissible purpose for the information and to record the identity of each person that receives a report on a consumer.

The consumer reporting industry is also unique because of the highly sensitive data involved and the manner in which the information is used. This information consists of credit reports and other detailed data bearing on consumers' confidential personal characteristics. Consumer reports benefit consumers as they enable consumers to purchase homes, buy cars, rent houses, cash checks and engage in many of the activities we take for granted in our day to day lives. At the same time, because this information is used to determine consumers' eligibility for credit, insurance, employment and similar essential economic transactions, consumers could suffer significant financial harm if the information is inaccurate.

In addition, because the data is so highly sensitive, consumers could be seriously harmed if the information is not kept confidential or is not properly used.

The Fair Credit Reporting Act provides for the confidentiality, the accuracy and relevancy of consumer report data. The FCRA protects the confidentiality of consumer reports, by permitting them to be disclosed only to those persons with a statutorily defined purpose for the information involved. The Fair Credit Reporting Act also contains provisions designed to promote the maximum possible accuracy of the information disclosed and it gives consumers the opportunity to see and correct the information on them.

The FCRA provides for notices to consumers when the information is used in a way that is adverse to a consumer's interest. Consumers also receive a notice summarizing their rights under the FCRA when they obtain their files from a consumer reporting agency. These notices and a comprehensive enforcement scheme assure the effectiveness of the FCRA in protecting consumers' rights in the confidentiality and accuracy of the data.

While these are the essential elements of the Fair Credit Reporting Act, it is a detailed and complicated statute. My written statement describes more fully the ways in which the FCRA works to protect the confidentiality, accuracy and use of consumer report information.

I want to emphasize that the Fair Credit Reporting Act is a unique statute, providing protection in a special area of the marketplace. It is unique because of the nature of the industry involved. It is unique because of the sensitivity of the information governed by the statute and it is unique because of the harm that improper use of the information can cause consumers. The FCRA is also unique because it balances the value of a healthy consumer

reporting industry against the potential harm caused by the misuse of the reported information and it carefully tailors its requirements and restrictions to this special industry.

For these reasons, I believe that while the Fair Credit Reporting Act works well in protecting consumers' privacy in the consumer reporting area, it should not be viewed as a paradigm for other privacy legislation in other industries Mr. Chairman, that concludes my opening statement. I'd be happy to answer any questions from you or other members of the subcommittee.

Mr. STEARNS. Ms. Fortney, thank you very much. I think your 25 years of experience will be useful for us, this country to develop another privacy bill.

[The prepared statement of Anne P. Fortney follows:]

PREPARED STATEMENT OF ANNE P. FORTNEY, PARTNER, LOVELLS

Mr. Chairman and Members of the Subcommittee, I am Anne Fortney. I am a partner in the Washington, DC office of the international law firm, Lovells.[1] Thank you for inviting me to participate in this Subcommittee's examination of existing federal statutes addressing information privacy. My testimony discusses the Fair Credit Reporting Act (FCRA)[2].

The FCRA governs credit records and similar personal information on consumers that is collected and reported by consumer reporting agencies. These records contain detailed information about consumers' credit accounts, such as outstanding indebtedness, credit limits, payment histories, foreclosures, judgments and bankruptcies. The records may also include income, employment, insurance data and even criminal arrests and convictions.[3]

Acting essentially as information clearinghouses, consumer reporting agencies[4] obtain consumer data on a regular basis from creditors, employers, insurers, government agencies, public records and similar sources. They then supply this information, upon request, to creditors, employers, insurers and others. In the past, most consumer reporting agencies were credit bureaus, providing credit reports. Today, consumer reporting agencies may also offer employment screening, tenant screening, check verification and similar information services.

Some consumer reporting agencies also prepare "investigative consumer reports." These reports, which are regularly obtained by employers and insurance companies, contain information about a consumer's character, lifestyle, morals, and general rep-

---

[1] My law practice concentrates primarily in the consumer financial services field, including the federal consumer protection laws and privacy. I have more than twenty five years' experience in this area. I have served as the Associate Director for Credit Practices at the Federal Trade Commission, have worked as in-house counsel for a national retail creditor and more recently have been engaged in the private practice of law. A copy of my c.v. is attached.

[2] 15 U.S.C. 1681 *et seq.*

[3] As evident from this description, consumer reports include more than just credit reports. A consumer report is any communication by a consumer reporting agency bearing on a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" which is used or expected to be used or collected for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance, for employment purposes, or for any other purpose authorized under the FCRA. FCRA § 603(d)(1); 15 U.S.C. § 1681a(d)(1).

"Consumer report" does not include information solely about transactions or experiences between a consumer and the person making the report. For example, if a bank reports about a consumer's payment history on a credit card issued by the bank, that is not a consumer report. The "transaction" or experience information is also not a consumer report when it is shared among corporate affiliates. In addition, corporate affiliates may share consumer report information if the consumer involved is notified that this information may be shared in this manner, and the consumer is given an opportunity to opt-out of its being shared and does not do so. In that case, the information involved is not considered a "consumer report" for most purposes of the Act. FCRA § 603(d)(2); 15 U.S.C. § 1681a(d)(2).

[4] A consumer reporting agency is "any person, which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." FCRA § 603(f); 15 U.S.C. § 1681a(f).

utation. The information reflected in these reports is generally collected through personal interviews with friends, neighbors, and associates of the consumer.[5]

The comprehensive consumer reporting network is an essential element of our consumer credit system, enabling creditors to make credit granting decisions quickly, accurately and efficiently. The benefits of this network include greater competition among creditors, lower credit costs for consumers and enhanced access to credit. The public also benefits when insurers, employers, landlords, merchants, banks, and others use the information to determine a consumer's eligibility for insurance, employment, a government license or for some other business transaction with the consumer (such as to cash a check or rent an apartment).

While the benefits derived from this information network are clear, it is also evident that consumers could be significantly harmed if this highly confidential, sensitive data were inaccurate, were freely disseminated or were to be misused. Inaccuracies in a consumer report could result in a consumer being denied credit wrongfully or being offered credit on less favorable terms. Inaccurate consumer reports could also result in denial of employment, insurance or important government benefits. Consumers could be substantially harmed if their consumer reports were obtained by former spouses, litigation opponents or others if they lack a legitimate purpose for the reports.

The FCRA was enacted to protect consumers from this kind of potential injury. However, because of the important public benefits derived from the consumer reporting network, the FCRA does not restrict the kind of information that is furnished to consumer reporting agencies and generally does not restrict the content of consumer reports.[6] Instead, the FCRA carefully addresses the potential consumer harm resulting from inaccuracies, improper access and misuse, and thus is designed to protect consumers in the accuracy, confidentiality and proper use of consumer reports. To ensure the protection of consumer data used in credit, employment, insurance, and other transactions, the FCRA imposes substantial obligations on credit bureaus, persons who furnish consumer data to credit bureaus, and persons who use consumer reports.

Enacted thirty years ago, the FCRA is remarkable in that it embodies many of the privacy concepts considered important today, including confidentiality, accuracy, relevance, notice, and access. It is important to note that the FCRA's original provisions were largely adapted from pre-existing voluntary guidelines of the consumer reporting industry, and the privacy concepts embodied in those provisions were carefully tailored to the special nature of the industry, the sensitive information involved and the significant manner in which it was used.

While the FCRA functions well for the consumer reporting industry, it should not be adopted as a paradigm for privacy legislation in other industries, where the information may be less sensitive and the uses to which it is put may be of less consequence for consumers.

CONFIDENTIALITY OF INFORMATION

The FCRA protects consumers' privacy by restricting the distribution of sensitive information maintained by consumer reporting agencies. Consumer reporting agencies may provide consumer report information only to persons[7] who intend to use that information for one or more of the "permissible purposes" set forth in the statute,[8] and no person may obtain or use a consumer report for any purpose unless the report is obtained for a permissible purpose.[9] Permissible purposes include determining a consumer's eligibility for credit, insurance, or employment.[10] Users of consumer reports must certify to consumer reporting agencies the purposes for which they intend to use reports,[11] and consumer reporting agencies must maintain procedures to ensure that they do not provide consumer report information to persons who do not have a "permissible purpose" to obtain such information.[12] The FCRA also effectively restricts the onward transfer of consumer report information once a user obtains the report.[13]

---

[5] FCRA § 603(e); 15 U.S.C. § 1681a(e).

[6] There are certain limitations on "obsolete" information, discussed below. *See* FCRA § 605; 15 U.S.C. § 1681c.

[7] The term "person" means any individual, government entity, or business entity. FCRA § 603(b); 15 U.S.C. § 1681a(b).

[8] FCRA § 604(a); 15 U.S.C. § 1681b(a).

[9] FCRA § 604(f); 15 U.S.C. § 1681b(f).

[10] FCRA § 604(a); 15 U.S.C. § 1681b(a).

[11] FCRA §§ 604(f), 607(a); 15 U.S.C. §§ 1681b(f), 1681e(a).

[12] FCRA § 607(a); 15 U.S.C. § 1681e(a).

[13] If a user of a consumer report regularly supplied consumer reports to an unaffiliated third party, that user could become a consumer reporting agency because of the Act's definition of

The FCRA recognizes that some businesses may obtain consumer reports for the purpose of reselling them to others. For example, mortgage reporting companies may procure reports from more than one credit bureau, and combine them into one report, deleting duplicative information. The combined report would be sold to a mortgage lender. The FCRA provides for confidentiality of that report in several ways. Because the combined report would be a consumer report, its contents would be subject to the same protections as other consumer reports. Moreover, because the mortgage reporting company is reselling the consumer reports that it obtains from the credit bureaus, it must certify to each credit bureau from which it obtains a report that it will resell the report only for a permissible purpose and must identify the end-user of the report.[14]

The FCRA also imposes restrictions on "prescreened" reports, limiting the information they may contain.[15] Moreover, consumer reporting agencies must give consumers the opportunity to opt out of receiving "prescreened" unsolicited offers of credit or insurance.[16] When consumer reports are used in connection with credit or insurance prescreening, the user must give the consumer a clear and conspicuous statement of the consumer's rights with each written solicitation and must maintain certain records with respect to the solicitation.[17]

In addition to limiting the use of consumer reports to those with "permissible purposes" and imposing other restrictions on use, the FCRA imposes obligations under specific circumstances, such as in the case of "investigative consumer reports."[18] Special obligations are also imposed on consumer reporting agencies and users of consumer reports when the reports are used for employment purposes.[19]

The FCRA also protects consumers' confidentiality by making it a crime for anyone to obtain a consumer report from a consumer reporting agency under false pretenses.[20] It is also a crime for an employee of a consumer reporting agency to knowingly and willfully provide a consumer report to an unauthorized person.[21] In addition, anyone who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose would be liable to the consumer reporting agency for actual damages or for $1,000, whichever is greater.[22] These provisions create an effective deterrent against deliberate misappropriation of consumer reports.

ACCURACY OF INFORMATION

Because of the ways in which consumer reports are used and the significance of their use in consumers' lives, accuracy is a key concern. Because consumer reporting agencies are the secondary source of the information they report, they must take steps to ensure that errors are not made in recording or transmitting data and to ensure that the information reported is not misinterpreted by the inquirer. However, given the billions of items of information transmitted electronically to and from consumer reporting agencies, perfect accuracy is impossible, and the FCRA recognizes this fact. For that reason, the FCRA does not impose strict liability on consumer reporting agencies for report inaccuracies. Rather, the statute requires consumer reporting agencies to follow "reasonable procedures to assure maximum possible accuracy of the information" they report.[23]

Recognizing that even accurate information may be misunderstood if it is not complete, the FCRA also requires consumer reporting agencies to disclose certain information when it pertains to the consumer reports they supply. Specifically, they

---

that term. *See* FCRA § 603(f); 15 U.S.C. § 1681a(f). The FCRA's intricate compliance responsibilities for consumer reporting agencies discourage users from assuming that burden of becoming a consumer reporting agency and thus prevent the onward transfer of consumer report information to those that do not have a permissible purpose.

[14] FCRA § 607(e); 15 U.S.C. § 1681e(e).

[15] FCRA § 604(c); 15 U.S.C. § 1681b(c). Prescreened consumer reports may contain only name and address, a unique identifier code (not the consumer's social security number), and other data that does not identify the relationship or experience of the consumer with respect to a particular creditor or other entity.

[16] FCRA § 604(e); 15 U.S.C. § 1681b(e).

[17] FCRA § 615(d); 15 U.S.C. § 1681m(d).

[18] FCRA § 606; 15 U.S.C. § 1681d. Before anyone may obtain an investigative consumer report, he must notify the consumer of the consumer's right to request a complete disclosure of the nature of the investigation requested.

[19] FCRA § 604(b); 15 U.S.C. § 1681b(b). For example, the consumer must have authorized in writing that the report may be obtained, and the user of the report must give the consumer an opportunity to review the report before taking an adverse action based on the report.

[20] FCRA § 619; 15 U.S.C. § § 1681q.

[21] FCRA § 620; 15 U.S.C. § 1681r.

[22] FCRA § 616(b); 15 U.S.C. § 1681n(b).

[23] FCRA 607(b); 15 U.S.C. 1681e(b).

must disclose the chapter of any bankruptcy they report (such as Chapter 7 or Chapter 13), whether a closed account was closed voluntarily by a consumer, and whether report information is disputed by a consumer.[24]

When the FCRA was enacted, obligations to assure accuracy of consumer reports were limited to consumer reporting agencies. Over time, however, it became evident that consumer report inaccuracies could also be due to errors by furnishers in providing data to these agencies. (Furnishers are, for example, banks that provide credit account payment histories.) For that reason, Congress amended the FCRA to impose certain duties on furnishers as well. These duties include furnishing accurate data, not knowingly reporting false data, correcting and updating data, and notifying consumer reporting agencies if consumers dispute the accuracy of the information they furnish.[25]

From the beginning, the FCRA recognized that consumers are in the best position to correct inaccurate information or require that it be updated. For that reason, the FCRA requires consumer reporting agencies to give consumers reasonable access to their files and to see all the information that could be reported on them.[26]

Because of the potential harm resulting from inaccuracies in consumer reports when the reports are used as a basis for declining applications for credit, employment, insurance or for similar uses, the FCRA requires users of consumer reports to notify a consumer when they take an adverse action based on his or her consumer report.[27] A similar notice is required when the adverse action is based on certain information that the user obtained from a corporate affiliate.[28] Consumer notice is also required when credit is denied or the charge for credit is increased based on certain information from a third party other than a consumer reporting agency.[29]

Consumer reporting agencies and furnishers of consumer information must reinvestigate information when a consumer disputes the accuracy or completeness directly to the consumer reporting agency.[30] If the information cannot be verified, it must be deleted.[31] If the dispute is not resolved to the consumer's satisfaction, consumer reporting agencies must allow consumers to include in their file a brief statement to the effect that the consumer believes the information to be incomplete or inaccurate.[32]

Consumer reporting agencies have special obligations with respect to the accuracy of public record data used for employment purposes which is likely to have an adverse effect on a consumer. (Examples of public record information include bankruptcies, DUI and other criminal arrests and convictions.)[33] For instance, consumer reporting agencies must maintain strict procedures to ensure that public record data is up-to-date and accurate, or they must notify the consumer of the person to whom the adverse information is being reported.[34]

RELEVANCE OF INFORMATION

The FCRA reflects a Congressional determination that, at some point, adverse information about a consumer's past credit history becomes so old that it should not be relied upon as an indicator of the consumer's present creditworthiness. To address this concern about reliance on "obsolete" information, the FCRA prohibits reporting certain adverse information that is more than seven years old. For example, civil judgments, charged-off accounts, or paid tax liens that are more than seven years old may not be reported. Statutory exceptions to this general rule permit unlimited reporting in connection with credit or insurance transactions for more than $150,000 and employment transactions for more than $75,000. In addition, bankruptcies may be reported for ten years, and criminal convictions are not subject to any time limit.[35]

Special relevance obligations are imposed on consumer reporting agencies with respect to "investigative consumer reports."[36] For instance, they may not reuse investigative consumer report data unless it is a matter of public record, is less than 3

---

[24] FCRA §§ 605(d)(e)(f); 15 U.S.C. §§ 1681c(d)(e)(f).
[25] FCRA § 623(a); 15 U.S.C. § 1681s-2(a).
[26] FCRA §§ 609, 612; 15 U.S.C. §§ 1681g, 1681j. However, credit scores need not be disclosed.
[27] FCRA § 615(a); 15 U.S.C. § 1681m(a).
[28] FCRA § 615(b)(2); 15 U.S.C. § 1681m(b)(2).
[29] FCRA § 615(b)(1); 15 U.S.C. § 1681m(b)(1).
[30] FCRA §§ 611, 623; 15 U.S.C. §§ 1681i, 1681s-2.
[31] FCRA § 611(a)(5); 15 U.S.C. § 1681i(a)(5).
[32] FCRA § 611(b); 15 U.S.C. § 1681i(b).
[33] FCRA § 613; 15 U.S.C. § 1681(k).
[34] *Id.*
[35] FCRA § 605; 15 U.S.C. § 1681c. Consumer reporting agencies must maintain procedures to ensure that they do not report obsolete information. FCRA § 607(a); 15 U.S.C. § 1681e(a).
[36] FCRA § 614; 15 U.S.C. § 1681l.

months old, or has been verified in the process of making the subsequent consumer report.[37]

ENFORCEMENT

The FCRA establishes an effective enforcement system based on notice of rights and obligations, federal administrative enforcement, state attorney general enforcement and private right of action.

The FCRA's notice requirements are comprehensive. Consumer reporting agencies must give consumers a summary of their rights whenever they disclose the contents of a consumer's file to the consumer.[38] In order to ensure that furnishers of information and users of consumer reports understand their obligations under the FCRA, the statute requires consumer reporting agencies to give them written notice of these obligations.[39]

The FCRA empowers the FTC, the federal banking agencies and other federal agencies to bring enforcement actions against consumer reporting agencies, furnishers of data, users of consumer reports, and any other person who violates the FCRA.[40] State attorneys general may also sue to enjoin FCRA violations and may sue for damages on behalf of their citizens.[41] The federal agencies and state attorneys general have all of the investigative power that they have under their organic or enabling statutes.[42]

The FCRA creates a private right of action against consumer reporting agencies, furnishers of data, and users of consumer reports. Consumers may recover actual damages for negligent violations and statutory damages for willful violations. Punitive damages may also be recovered as allowed by the court. Successful litigants may also recover attorneys fees.[43]

STATE PREEMPTION

The FCRA provides for limited preemption of state laws. Generally, the FCRA does not preempt state laws governing the collection, use or distribution of any information, except to the extent that those state laws are inconsistent with the federal statute.[44] In addition, the FCRA preempts state laws with respect to the following areas: prescreening (§§ 604(c) and (e)) and notices contained in solicitations to prescreened consumers (615(d)), investigation of consumer disputes (611), duties of persons who take adverse action based on consumer reports (§§ 615(a) and (b)), content of consumer reports, and duties of persons who furnish information to consumer reporting agencies (623).[45] This limited preemption may sunset on January 1, 2004 if states enact new laws after that date and if the state law explicitly provides that the provision is intended to supplement the FCRA and the state law gives greater protection to consumers than the FCRA.[46]

UNIQUENESS OF THE FRCA

As I have described, the FCRA uniquely governs the confidentiality, accuracy, and relevance of consumer credit information and similar highly confidential data. The FCRA restricts the disclosure of this highly sensitive information to those individuals and companies with specific permissible purposes. The FCRA establishes requirements for consumer reporting agencies and furnishers of data to assure the maximum possible accuracy of the information. Because of the vast quantity of data involved, the FCRA recognizes the potential for error and creates mechanisms for correcting errors and eliminating inaccurate information. The FCRA also imposes time limits for clearing old data from consumer records, thus allowing consumers to "get well" after financial difficulties.

The FCRA recognizes that faulty credit reports could seriously impact the ability of consumers to purchase a house, acquire a car, cash checks, or conduct many of the other financial activities we take for granted in this country. On the other hand, the FCRA recognizes the value of the consumer reporting industry in effecting quick credit checks, accurate sharing of crucial financial information, and identifying indi-

---

[37] *Id.*
[38] FCRA § 609(c); 15 U.S.C. § 1681g(c).
[39] FCRA § 607(d); 15 U.S.C. § 1681e(d).
[40] FCRA § 621; 15 U.S.C. § 1681s.
[41] FCRA § 621(c)(1); 15 U.S.C. § 1681s(c)(l).
[42] FCRA § 621; 15 U.S.C. § 1681s.
[43] FCRA §§ 616, 617; 15 U.S.C. §§ 1681n, 1681o.
[44] FCRA § 624(a); 15 U.S.C. § 1681t(a).
[45] FCRA § 624(b), 15 U.S.C. § 1681t(b).
[46] *Id.*

viduals who are bad credit risks. Thus, the FCRA is a balanced statute, protecting individuals while allowing the proper functioning of an industry that is essential to this country's economic machinery. It is important to remember that the original provisions of the FCRA were derived from industry voluntary standards, which allowed the law to incorporate reasonable business practices.

The FCRA is a unique statute, providing protection in a special area of the market place. It is unique because of the sensitivity of the information governed by the statute and unique because of the harm that improper use of the information could cause consumers. The FCRA is also unique because it has balanced a healthy consumer reporting industry with necessary protections for consumers.

I caution that this effective law for the consumer reporting industry should not be adopted as a paradigm for privacy legislature in other industries. The unique sensitivity of the information covered by the FCRA and the serious harm that could result from improper use of this kind of information are generally not duplicated in other industries.

Mr. Chairman, I thank you for the opportunity to provide this information to the Subcommittee.

Mr. STEARNS. Mr. Fischer?

STATEMENT OF L. RICHARD FISCHER

Mr. FISCHER. Mr. Chairman, members of the committee, my name is Richard Fischer. I'm a partner in the law firm of Morrison & Foerster. Like Anne, I've worked in this area for some time, nearly three decades. I'm also the author of a leading treatise in this area, the Law of Financial Privacy. I'm very pleased to be here. I have an easier task. I've been asked to address a recent statute, one more familiar with this group, the Gramm-Leach-Bliley privacy provisions.

But first, I want also to applaud you and the committee on this series of hearings. As someone who has spent three decades on privacy issues, I've learned one thing. Privacy seems deceptively simple, but it's the most complex issue that I've ever worked on.

In terms of Gramm-Leach-Bliley, it establishes the most comprehensive financial privacy requirements of any Federal legislation ever enacted. It requires each financial institution to provide every customer with a written statement of its policies for protecting consumer privacy. In addition, every financial institution must give its customers the opportunity to prohibit, that is to opt out, of the disclosure of information to third parties beyond a series of exceptions that are set forth in the statute itself. These requirements become fully effective on July 1 of this year, that is in just 88 days.

Many financial institutions, however, have provided customers with privacy policies well before Gramm-Leach-Bliley. But the new law has required financial institutions, in fact, every institution, to reassess its policies and to implement extensive compliance programs to satisfy the Act's new notice and opt-out requirements.

For larger institutions, compliance has been a multi-phased effort involving literally hundreds of individuals throughout the organization. Both the scope and intensity of these efforts can only be described as Herculean. In my experience, no other piece of consumer legislation has ever engendered or required this magnitude of response.

Financial institutions have had to fully examine their information practices that flow into and out of financial institutions; make difficult business judgments attempting to weigh possible consumer privacy concerns against the efficiencies and consumer benefits of

using this information; and, establish their policies to set forth this judgment.

Financial institutions have developed privacy notices explaining their policies to customers, and are not in the process of putting into place programs to ensure that employees adhere to these policies in a rigorous way.

This has also been quite a competitive process. I have reviewed literally scores of privacy policies and they vary greatly. Many financial institutions are going beyond the requirements of the Gramm-Leach-Bliley Act. They're also making extra efforts to explain their policies to their customers and to explain, in particular, the benefits of information sharing to those customers. In many cases, institutions have further reduced the information available to others including their servicing companies. And in virtually all cases, institutions have increased controls over the use and the disclosure of information.

As a result, even though the Act is not yet fully effective, it's already increased the historically high level of confidentiality employed by financial institutions.

But this is only the beginning. Under the Act itself, companies receiving information from financial institutions must also ensure that the use of that information is limited to the purpose for which it's provided. This requires segregation of information according to the purpose for which it was received, tagging of information to identify its origin and permissible uses.

It is far too early to assess the full effect of Gramm-Leach-Bliley on financial privacy. Consumers are just beginning to receive their initial privacy notices. Tens of thousands of financial institutions will be mailing billions of privacy notices to their customers over the course of the next 3 months. And I did say billions of privacy notices. Most consumers will receive 20 or more notices in this context. The notice will evidence a variety of choices and in fact, how consumers exercise those choices will tell us an awful lot about consumer privacy preferences and in particular about their appreciation of the benefits of information. Financial institutions also will be watching the actions of their competitors, because in fact, this has become a very, very competitive issue. In other words, market transparency and the role of market forces in shaping privacy practices will dramatically increase over the next several months.

Thank you again for the opportunity to appear here and I also would be pleased to answer any questions.

[The prepared statement of L. Richard Fischer follows:]

PREPARED STATEMENT OF L. RICHARD FISCHER, PARTNER, MORRISON AND FOERSTER

My name is L. Richard Fischer. I am a partner of Morrison & Foerster and I practice in the firm's Washington, D.C. office. I have nearly three decades of experience in advising banks and other financial services companies on retail banking matters, including privacy, and I am the author of the leading treatise on this subject—*The Law of Financial Privacy*. I am pleased to have the opportunity to appear before you today to address the issue of information privacy and the requirements of the recently enacted Gramm-Leach-Bliley Act.

As you are aware, the Gramm-Leach Bliley Act (the "GLBA") established the most comprehensive financial privacy provisions of any federal legislation ever enacted by Congress. The GLBA requires each financial institution to provide every customer with a clear and conspicuous statement of the institution's policies and practices for protecting the privacy of customer information. In addition, each financial institution must provide its customers with notice, and an opportunity to prohibit, or opt

out of, the disclosure of information to nonaffiliated third parties. Under regulations promulgated to implement the GLBA, these requirements become fully effective on July first of this year. Currently the financial services industry is in the midst of readying itself for this July 1, 2001 effective date. Not only are financial institutions putting in place programs to comply with the notice and opt out requirements of the GLBA, but they also are reviewing and revising their corporate information policies and practices. In fact, it simply is not possible for a financial institution to craft a privacy notice without first conducting an inventory of its current information practices and shaping those practices prospectively in a manner consistent with that privacy notice. As a result, financial institutions have been reviewing, and where appropriate restructuring, their relationships with third party servicers and other companies to further limit the disclosure of information about consumers, and to increase their control over information when it is disclosed.

The full effects of the implementation of the GLBA will not be apparent for some time. Nevertheless, from first hand experience in working with a wide variety of financial institution clients, I can attest that the changes in market practices that already have resulted from the GLBA have increased the high level of confidentiality with which financial institutions have historically treated their customer information. Further, the privacy notices required by the GLBA, which consumers have already begun to receive, can be expected to raise consumer awareness of privacy-related issues. This will enable market forces to further shape information practices to reflect even more closely consumer expectations.

THE GRAMM-LEACH-BLILEY ACT

The GLBA applies to a broad range of financial institutions. It sweeps within its coverage not only traditional banks, securities firms, and insurance companies, but also all other providers of financial products and services as defined under section 4(k) of the Bank Holding Company Act. As a result, retailers issuing credit cards, money transmitters, check cashers, mortgage brokers, real-estate settlement services, appraisers, tax preparation services and even online companies that offer aggregation, funds transfer or payment services are all financial institutions under the GLBA.

Because of the GLBA, no company that provides financial products or services to individuals for personal family or household purposes may provide non-public information about those individuals to a nonaffiliated third party for any purpose outside of a specific list of exceptions without first giving the individuals an opportunity to opt out of that disclosure of information.

In addition, at the time of establishing a retail customer relationship with an individual, and at least annually thereafter throughout the entire life of that relationship, a financial institution must provide the customer with a clear and conspicuous disclosure of the institution's policies and practices with respect to the disclosure of personal information to both affiliates and nonaffiliated third parties. This detailed notice must describe, among other things, the categories of information collected by the institution, the categories of information to be disclosed, the categories of persons to whom information may be disclosed and the institution's policies for protecting the confidentiality and security of the information. And this disclosure obligation applies even if the financial institution discloses no information to third parties. Where information is disclosed to third parties, it is subject to reuse and redisclosure limitations to ensure that the use to which information is put is consistent with the purpose for which the information was disclosed.

These statutory requirements are implemented by regulations adopted by seven federal agencies, including the bank supervisory agencies, the Securities and Exchange Commission and the Federal Trade Commission, as well as by rules adopted by the States for insurance companies.

Many financial institutions adopted privacy policies and communicated them to their customers well before the adoption of the GLBA, and they have a long history of treating customer information as confidential. However, the specific requirements of the GLBA and the implementing agency regulations have required all financial institutions to reassess their policies and practices concerning the collection and use of customer information, and to implement compliance programs to satisfy the new GLBA requirements for notices and opt-outs.

THE IMPLEMENTATION EXPERIENCE

I have been deeply involved in advising a wide variety of financial institutions on their efforts to comply with the GLBA. For larger institutions, compliance has been a multiphased effort involving individuals from throughout the organization, including its policy, operations, information management, legal, and compliance functions.

Both the scope and intensity of these efforts have been Herculean; so will the resulting communication onslaught—tens of thousands of financial institutions sending billions of privacy notices to consumers throughout the country. In my experience no other piece of consumer legislation has engendered or required a response of this magnitude.

Financial institutions have conducted comprehensive surveys of every aspect of their practices concerning consumer information and evaluated those practices in terms of the expectations and preferences of their customers. They have made difficult business judgments weighing the possible privacy concerns of their customers against the efficiencies and consumer benefits of using customer-related information to identify and respond to the needs of those customers,[1] and established policies and practices to reflect those judgments. Financial institutions have developed notices explaining these policies and practices to their customers, and have put in place programs to ensure that the notices are delivered to customers and that their employees adhere to these policies and practices, not only in spirit, but in a rigorous way.

This also has proved to be a highly competitive process. Although I have reviewed scores of privacy notices, few look alike. Financial institutions have designed their privacy notices to address the preferences and concerns of their customers as they perceive them. Some financial institutions are even establishing tailored policies and providing special notices for different types of financial products or programs in order to ensure that the privacy expectations of those customers are met. Many financial institutions have tested their policies on focus groups in order to determine whether they have assessed their customer preferences correctly, and some of these institutions have had to return to the drawing boards when they concluded that they did not access those preferences correctly.

Even where information about consumers will be shared with servicers and other third parties, many financial institutions are going well beyond the regulatory requirements for disclosure to explain their practices to consumers and to explain how consumers benefit from those practices. In many cases institutions have curtailed the flow of information and restructured business relationships to limit the disclosure of information about their customers, particularly to nonaffiliated third parties. In virtually all cases, the process has lead to increased controls over the use and disclosure of information about consumers, even where that information is necessary to service and maintain customer relationships.

But the efforts to date are only the beginning. Because of the importance that the GLBA places on limiting the subsequent use and redisclosure of information about consumers, financial institutions and the outside companies that assist them in servicing their customers, must review and revise their outsourcing agreements and implement procedures to ensure that customer information is used only in accordance with applicable privacy policies. They also must ensure that they comply with the reuse and redisclosure limitations in the GLBA and the implementing agency regulations. In many cases, this requires the segregation of information according to the purpose for which it was received, or separately tagging information to indicate its origin and permissible uses.

GOING FORWARD

At this time, it is far too early to assess the full effect that the GLBA will have on financial privacy. Consumers are just beginning to receive their initial privacy notices for their existing customer relationships. Most consumers will receive several notices—perhaps 20 or more privacy notices each. These privacy notices will evidence a variety of choices with respect to the sharing of information about them with third parties. How consumers exercise those choices will tell us much about consumer privacy preferences and their appreciation of the many benefits of information sharing. In addition, financial institutions will be watching the actions of their competitors, as well as the responses of their customers, and then carefully revising or adjusting their policies accordingly. In other words, market transparency—and accordingly the role of market forces in shaping privacy practices—will increase dramatically over the next few months.

---

[1] Recent studies have begun to explore and detail the consumer benefits of collecting and using consumer information, including a survey by Ernst & Young of the banking, insurance and securities firms that are members of the Financial Services Round Table (A copy of this study is attached to my testimony). Other benefits are catalogued in a recent paper prepared for the American Enterprise Institute by Professor Fred H. Cate of the Indiana University School of Law, entitled *Privacy in Perspective* (a copy of the paper also is attached to my testimony). [The study and the paper are available on the Committee on Energy and Commerce website.]

Mr. STEARNS. Thank you, Mr. Fischer.

Mr. Richard Smith of the Privacy Foundation, the Chief Technology Officer, we're pleased to have your opening statement.

STATEMENT OF RICHARD M. SMITH

Mr. SMITH. First off, I'd like to thank the committee and the chairman for the opportunity to speak today. I am not a lawyer, so I'm going to be talking more about technology, but I was asked to talk about the TiVo service in a recent privacy advisory put out about it. But I think what it really illustrates here is how new technology is going to be putting pressure on existing laws. I'm a technologist and clearly we can all see the Internet and what it's done for privacy and also cell phones.

What we're seeing now with services like TiVo is that some of these Internet surveillance techniques that are used are coming to our consumer electronic devices. TiVo is basically a VCR on steroids, if you will. It allows, it has a computer and it's used to store TV programs on a hard disk. And it's what VCRs should have been 20 years ago, rather than having a blinking light saying what time is it, this device allows us to very easily record TV programs. And it does this by having electronic program guide. So all we do is if we just point our remote control at the electronic program guide, it allows us to record our TV programs. Now what's interesting about this VCR is the fact that it has a telephone connection, that it has to have a telephone connection in order to get the electronic program guide information. So at the Privacy Foundation, whenever we see a telephone line, we wonder well, what kind of information is going back and forth. And so we took a look at actually sniffing or listening in on that conversation between a TiVo box and the TiVo service to learn the information transfer in both directions. So of course, we saw the electronic program guide information coming down, but we also saw other information going back, such as the internal temperature of the box and keys that are being pressed on the remote control and also viewing information of what programs we had watched on our VCR unit. And we found this very interesting.

So we then went and took a look at in the TiVo service to try to understand what kind of notice and choice provisions TiVo was giving to consumers about this action. So I'll just read here real briefly a statement from the manual. It says "Will the TiVo service collect information about my viewing habits?" And this is in the manual that came with the box and I'll skip over some of the initial things that were said, but the sentence that really caught our eye says, "Unlike the Internet, all your personal viewing information remains on your PTP receiver in your home." PTP receiver being the TiVo box. To our mind, that statement contradicts directly what we had seen. But if you go back and read the privacy promise that they have in the manual which is more of a legal agreement, it's about five pages long, they actually go through and describe what they actually mean here. And the issue here gets down to—they give a very mixed message. The TiVo service and the privacy policy, if you read it, if you go through those five pages, you'll learn that they anonymize this viewing information. So even though this information is about the TV programs you watch, they strip off any

names or addresses associated with it. But you would never really know that if you simply read the operational instructions that came with the device.

So from our perspective, there was a real problem here of properly alerting consumers about how information is being used. And this is a device that's being put in our house and it's one of the first devices that are going in our house this way besides our home computers that are going to report back information. And so we felt that in our advisory that there had to be a much better way of doing this, to let consumers know so that they trust these devices that we're dropping into our houses. And we said well, this is a TV device, it hooks up to the TV. Why can't the TV screen say what it's doing? So what we recommended to the company that they put a notice on the TV screen at the time you set up the box saying we'd like to have the TiVo service be better and one way we can do that is learn about what TV shows you watch. Would you like to participate in this program, yes or no? And we thought that a much better approach than the current approach that we have here with the TiVo being kind of doing it on the sly.

The TiVo debate is like a lot of the other privacy debates that we've had of opt-in and opt-out. They do offer an opt-out, you know, which is described in that five-page legal agreement. It's kind of funny that our VCRs now need a five-page legal agreements to describe how they work. But in there, there's an 800 number you can call up and opt-out of this collection process. Again, there's a TV set, we felt that that was much more appropriate, just a button to push on the TV set. We called up and it took close to 15 minutes to opt-out of this data collection practice on the time that we did. So again, we look at fairness issues here with these devices.

We're not opposed to necessarily the device wants to collect this information as long as it does it with adequate notice, an important notice to really let a consumer know what's going on and the ability to opt-out.

Now TiVo, we just look at the tip of the iceberg. What we really see over this next decade is consumer electronics becoming web-enabled and using the Internet to communicate back information. So we don't look at it this is just a TiVo issue, but the on-going issue of digital television, digital cable.

Thank you very much for this opportunity. I'd be happy to answer questions.

[The prepared statement of Richard M. Smith follows:]

PREPARED STATEMENT OF RICHARD M. SMITH, CHIEF TECHNOLOGY OFFICER, PRIVACY FOUNDATION

The Privacy Foundation today released its first Privacy Advisory regarding a set-top box: the TiVo personal video recorder. It seems clear from our research that many of the privacy issues dogging the Internet (tracking individual behavior, opt-in/opt-out, and murky privacy policies) are headed straight for your TV set.

The best way to describe TiVo is as a VCR on steroids. Rather than using video tape to record TV programs, it uses a hard disk, with up to 60 hours of recording time in one model. The box is controlled by an internal computer that comes with sophisticated software, along with an electronic programming guide, that makes it easy to identify and record TV programs and watch them later. You can even program it to record shows up to two weeks in advance.

TiVo has the TV industry very concerned because TiVo viewers can easily fast-forward through ads. But TiVo's investors and partners include some of the biggest

players in the game: NBC, AOL Time Warner and Nielsen Media Research. I'll tell you what I think is going on with them later in the column.

But first, the snoopy part.

Because a TiVo box plugs into the phone line, we were very interested in learning what our TiVo box says when it phones home to TiVo. The phone line is primarily used to download TV schedules to the box, but it can also upload information back to TiVo. In particular, we wanted to find out if it reports back to TiVo what we are watching on TV. We also wanted to know out how up-front TiVo is in telling subscribers about any tracking that might be done. This meant reading marketing literature, TiVo manuals, terms of service agreements, and TiVo's filings with the SEC.

To read the advisory in full, click here. I'll summarize some of the key findings below.

To answer our first question, "Does a TiVo box spy?," Dr. David Martin, the technical lead at the Privacy Center at the University of Denver, created a modem sniffer set-up that allowed him to watch all the data that passed back and forth between his TiVo box and TiVo servers. He found that the TiVo box was very talkative. He saw that it was sending back the following types of information back to the TiVo:

- His customer ID number for the TiVo service
- Times and dates when he was using the TiVo box
- The internal temperature of the box
- Some button presses on the TiVo remote control
- Information about what TV programs he was watching

Much of the data being sent back looked like telemetry from a NASA rocket launch. Pretty amazing stuff for a consumer electronics gadget! Dr. Martin then put on his detective hat and figured out how all this data was organized. He discovered that the TiVo box actually sends out two separate files during its nightly phone call.

When comparing the data collected by TiVo with its stated privacy policies, Dr. Martin drew the following conclusion: "TiVo receives all of the information necessary to attribute the viewing information to a particular subscriber during this phone call but gives no indication of this fact in any of its documentation."

What's going on? Part of the mystery is solved in the "TiVo Privacy Promise" in the back on the user manual. Basically, TiVo claims it doesn't use "personal viewing information" that could be tied to a particular individual. However, it does use "anonymous viewing information," which is that same information, stripped of personal identifiers, and aggregated for data mining purposes. A phone call to TiVo executives confirmed that this is how it works. TiVo allows subscribers to opt-out of providing "anonymous viewing information," though the company admits that only a small percentage of subscribers do that. Probably that's because TiVo doesn't exactly promote this opt-out feature in their marketing materials and legal agreements.

My bottom line here is that TiVo isn't playing very fair with their customers, who number more than 150,000. Even if it is "anonymous" information about what TV shows people are watching, TiVo needs to do a better job of explaining what is going on. Why not use the TV screen itself? During system setup the TiVo box could show a couple of screens that explain how TiVo does anonymous tracking. Then they could ask consumers if they would like to participate in this program or not. Seems pretty simple to me!

But what is TiVo's goal in collecting all this data, particularly given its alliances with big media partners? I think TiVo is collecting "anonymous" viewing information as a bargaining chip in their negotiations with the TV industry. By collecting this data, TiVo knows more about the TV industry's customers than they do. TiVo's viewing data is more easily quantified than Nielsen's statistical samples, which is one reason that Nielsen is partners with TiVo in an opt-in viewer survey analysis.

Yet, TiVo acknowledges that they really aren't making much money from the anonymous data today. And, due to technical issues and the uncertainty of viewer acceptance, it is doubtful that TiVo will be able to effectively use such information to target commercials to individual viewers, even though this was one of their original ideas.

One potential payday would be if TiVo collected specific viewer information, tied to demographics and psychographics, then sold that data for a variety of direct marketing purposes. But company officials, including co-founder and CTO James Barton, claim that is not going to happen. One of TiVo's legal disclosures gives a little more wiggle room for the future, stating, "Under our current policy, we do not access [viewer] data or release it to third parties."

The privacy issues around TiVo may soon apply to a range of consumer electronics devices. Are our TV sets, digital cable boxes, satellite TV receivers, and MP3 players all going to becoming data collection devices for marketers and advertisers? I cer-

tainly hope not. Internet-enabled devices should be designed to minimize the amount of data they send back about us. If companies want to spy on us, they are going to have to make it very clear what's going on and ask if it is okay.

If companies try to slide snooping devices into our homes on the sly, I think they'll only hurt themselves. If consumers can't tell which Internet-enabled devices will spy and which ones won't, maybe they won't buy them at all.

Mr. STEARNS. Thank you, Mr. Smith.

Let me start with my set of questions and first to Richard Fischer. You had mentioned something about the Gramm-Leach-Bliley Act and as a result thereof, companies have curtailed the flow of customer information to third parties, even beyond what is required by the Act, I think you indicated.

How has that changed, impacted the customer for good or for bad?

Mr. FISCHER. That, Mr. Chairman, is a great question because that's to be seen as this plays out. But just to give you an example, the Gramm-Leach-Bliley Act allows you beyond the exceptions to share information with third parties so long as you give the consumer notice and a chance to opt out. There are many financial institutions that have said we don't want to do that. In other words, we're going to cut back even though we have the ability under the Act to disclose that information to the third parties, we would have to give the notice to opt-out and we would prefer not to have to give a notice to opt-out at all, therefore, we're not sharing. And if you look at it from a privacy perspective, you could say that's good, that's information not going out to a third party, but as you indicated in your opening statement, it really is a cost benefit analysis always because what it really means then is somebody isn't getting an opportunity in this context because the information is not going out. As we see that balance, the Gramm-Leach-Bliley Act and particularly the regulations could have permitted a cookie cutter approach to disclosures, but that's not has happened. The disclosures are really all over the place and I think that as consumers receive these things, look at them, make decisions, we'll see what it means.

Mr. STEARNS. Gramm-Leach-Bliley At, do you think Congress should do something to change or amend the Act? Just yes or no?

Mr. FISCHER. Presently, I think the answer is no.

Mr. STEARNS. Mr. Smith, in your TiVo, they're getting information through the telephone line, but I have a television where I just push a button and it gives the entire programming for the day and I assume that's coming through transmission to the television and not through the phone line. Are all the TiVos set up that they are connected to a telephone line?

Mr. SMITH. Yes, that's correct. And the reason they go through a telephone line is different cable systems and satellite systems have different ways of sending down the electronic program guide, so TiVo only wants one way to get them and so they go through the phone line.

Mr. STEARNS. And so it costs the customer money? It's just a local call. Do you get a separate telephone line for a TiVo?

Mr. SMITH. No, it makes the phone call like at 2 in the morning, so it uses your standard phone line.

Mr. STEARNS. I see.

Mr. SMITH. There's a subscription service for TiVo. It's $10 a month, basically.

Mr. STEARNS. I see. If we enact comprehensive privacy laws, should this privacy law pre-empt all other privacy laws and if not, what laws should be kept? Are you capable, maybe some of the other panel can answer this, but it seems to me that there's probably conflicting privacy laws and which laws should be followed?

Mr. SMITH. Well, I'm not a lawyer, so on the preemption question, that's a tough one. Sometimes it's appropriate, sometimes it's not. I just—I'll get a lawyer to get an answer for there.

Mr. STEARNS. Yes. Ms. Fortney, do you want to try and take that or Mr. Fischer, either one?

Mr. FISCHER. If you're looking at enforcement, Mr. Chairman, I think that multiple laws are terrific because as you said earlier, actually, Mr. Towns, if this was you, if you had an issue like this and somebody is violating the statute, it ought to be enforced.

When you're talking about substantive disclosures, I think preemption is essential. The notice that I talked about now is 2 to 6 pages. If you have multiple additional disclosure to be included, they really become worthless.

Mr. STEARNS. To think that in 1 year consumers are going to receive over 20 separate notices on privacy. That just seems like an overkill, in my opinion.

Mr. FISCHER. Congress decided that education and transparency was important here.

Mr. STEARNS. Right.

Mr. FISCHER. And the only way that you can do that is to allow notices across the broad range, all financial institutions.

Mr. STEARNS. Who can understand that, the average consumer?

Mr. FISCHER. That's a good question, Mr. Chairman. I think what it's going to come down to are those who are seriously concerned about privacy, will look at these carefully. If you look at those who are not, frankly, in that context, I think what Congress will come back to, after we go through this process is an alternative for others which is much shorter.

Mr. STEARNS. Especially those people who are not paying attention and could care less. Just worrying about their car starting in the morning, that's not going to be something they read too carefully.

Ms. Fortney, you concluded your statement by saying "I caution that this effective law for consumer reporting industry should be adopted as a paradigm for privacy legislation in other industries." You added that "the unique sensitivity of information covered by the FCRA and the serious harm that could result from proper use of this kind of information are generally not duplicated in other industries."

Would you care to comment on that statement because we're looking for those kind of statements which are all inclusive and emphatic, so that we can work off of them.

Ms. FORTNEY. Okay, I'd be glad to add to what I just said. As I indicated, the consumer reporting industry is unique in several respects and I think we need to focus first on the nature of the information involved. Consumer reports contain highly detailed information about consumers' credit records and other very sensitive financial information. But perhaps even more importantly is the way in which that information is used because the information is used

in a way that can determine whether a consumer is able to purchase a home, get a job, get insurance and other really very crucial economic transactions that consumers need to enter into. If the information is misused, then that information can have a very immediate serious negative impact on consumers' lives. I think in contrast to a lot of the information that we're discussing generally in this area where we're talking about the use of information for marketing purposes, or the use of information for similar purposes that have less dire economic circumstances, that it's not appropriate, it would not be appropriate to take a statute that is as comprehensive as the Fair Credit Reporting Act and try to apply it across the board to all other industries.

Mr. STEARNS. My time has expired. Mr. Towns?

Mr. TOWNS. Thank you. Let me begin with you, Mr. Fischer. You talked about the financial institutions going to implement privacy provisions of the Gramm-Leach-Bliley Act. It is my understanding the situation pertaining to insurance is not so bright. The National Association of Insurance Commissioners has adopted a model regulation for the states to implement which would require insurance company complies with these privacy provisions. It's my understanding that the State of New York is the only State so far to have implemented this model regulation entirely.

Mr. FISCHER. Mr. Towns, there are a handful of other states that have taken that step, but you're absolutely right and no industry has it more difficult right now than the insurance industry in complying with Gramm-Leach-Bliley. We do represent insurance companies as well. For banks, for example, there's one set of regs to deal with. For insurance companies, they could end up with 50 sets of laws that are quite different and 88 days left for compliance, the law applies to the insurance companies and you're absolutely right, sir, in many states there's no guidance yet.

Mr. TOWNS. What are your expectations? How many states by the end of the year do you feel would be in compliance? Do you have any idea? I know—based on your experience.

Mr. FISCHER. I think that you will find that one way or the other that you'll have at least three quarters of the states with regulations in place by the end of the year. If we're fortunate, it could be closer to 45 to 48 of the states, but there will be some stragglers.

The good news is it will be the State insurance commissioners that will be enforcing that. It's very difficult for somebody to try to force a law that they haven't given you guidance on yet. The bad news is there are still private plaintiffs out there that can enforce it after July 1.

Mr. TOWNS. How many of these would you expect to include the protection of medical information which I think is very, very important?

Mr. FISCHER. I think that you will see eventually all of them. Some of them have a cross reference to HIPAA so that you don't have to comply with conflicting guidelines, but I think in time you'll find, maybe not this year, that all of the states will cover medical information because the State insurance commissioners are coming to the same conclusion you have about the sensitivity.

Mr. TOWNS. Thank you. Mr. Lamb, AT&T operates a cable service, am I correct?

Mr. LAMB. Yes.

Mr. TOWNS. It must definitely comply with the Cable Act, am I correct on that?

Mr. LAMB. And we do.

Mr. TOWNS. Are you familiar with the privacy conditions the FCC put on its approval of the AOL-Time/Warner merger?

Mr. LAMB. Generally familiar but because they didn't apply to us I didn't study them in detail.

Mr. TOWNS. But Time/Warner had to actually stipulate in writing that it would provide the Cable Act privacy protections which require disclosure and an opt-out, opt-in, I'm sorry, for the collection of—dissemination of personally identifiable information of which are codified in Section 631 of the Communication Act to all its customers, not just its customer cables. Are you aware of that?

Mr. LAMB. I did not follow that, no.

Mr. TOWNS. Do you agree then with the FCC's imposition of this requirement?

Mr. LAMB. The issue really is—when you ask whether I agree, beside the merger, is that a good rule for the cable industry, perhaps or for the information communications industry, once they go beyond the——

Mr. TOWNS. I'll accept that. But go ahead, answer that.

Mr. LAMB. And I would say there is no one size fits all. The consumer concerns vary dramatically by industry. The industry practices, there is a history of high privacy compliance in telephony that frankly is not the case in on-line. The on-line industry has made great strides in the last 2 years, but there is no reason to think that either consumer concerns in one industry are the same or that the need for a fix or a solution is the same from one industry to another.

Mr. TOWNS. This is a very difficult situation as you know and I think that we want to move very cautiously and we want to sort of make certain that we touch every area and that's the reason why I raise those questions. It's not to—no more than to try to do what's right because I don't want to be involved in a situation where we do something and then a month from now we come back and realize—we have to come back and try and do something else. We want to try to move very carefully and slowly and get it right. That's the reason I'm raising this question and it's not a trick question in any way.

Mr. LAMB. No sir, I agree. We share your goal. All responsible companies across industries should be telling their customers how they use private information. The only question is how to get to that place.

Mr. TOWNS. My time has expired. I just want to ask one question to——

Mr. STEARNS. By unanimous consent. Go ahead.

Mr. TOWNS. Mr. Smith, let's say a criminal investigation is being conducted into a series of sexual assaults. TiVo cable have given law enforcement personnel all TiVo's home viewers serial numbers that viewed certain types of sexually explicit programs in a given location during a given period of time. And let me just add while I have this chance, what TiVo calls anonymous information in-

cludes not only viewing information, but also the home viewers' TiVo serial number. Is this not correct?

Mr. SMITH. No, the serial number would not be. That's personally identifiable because it's tied to your name and address.

So in the case, the way the service works today, they could find out well, there's a thousand people watching sexually explicit movies, but they couldn't really tie it back to who they were. Now they do have a new marketing program in place where they do want to match up with what you watch on TV and your name and address. And in that case, customers are putting themselves, data is being collected about them that used to not be collected. Five years ago, our TV sets didn't remember what we watched.

So if you choose to participate in that program whenever TiVo chooses to release it, there are some issues there that that could end up in court, either in civil or criminal cases.

Mr. TOWNS. Thank you, Mr. Chairman.

Mr. STEARNS. The vice chairman of the committee, Mr. Deal.

Mr. DEAL. Thank you. This has been a very interesting dialog here and reading the testimony that you have submitted. In listening to this whole issue of privacy, I can't help but be reminded of a flashback to a scene that all of us have lived on the playground as children which somebody asks a question and the response was "it's none of your business" to which the next response was "well, I'm making it my business."

It seems to me that the question has to be asked here why are so many people making it their business to know something about people that perhaps they don't want them to know? And certainly none of us would suggest that every consumer is an exhibitionist to the extent that he wants everything that he consumes to be known to everybody and certainly I don't think any of us would imply that all businesses are voyeurs who want to be Peeping Toms knowing everything about everything.

Mr. Fischer made the statement and our chairman alluded to this patchwork quilt that we have now in terms of regulatory processes as being issue and industry specific type regulations and that's the nature of the drafting of the legislation up to this point. But as I listen to your testimony, it seems that the information gathering process has primarily two focuses. One, that is as Mr. Fortney points out, in consumer credit line information, information that a business person needs to know in order to make a solid business judgment about a creditor purchase transaction that they may be a party to, with an unknown consumer for the protection of the industry that is engaging in that.

The second seems to be in its general nature that of being able to utilize information for further marketing purposes and several of you, of course, have alluded to that.

Are there other general areas where this information is needed or is used and if so, have we touched on the regulatory process that relates to them and second, if those are the two generally broad categories, we seem to have addressed the one rather well as Ms. Fortney outlined in existing regulatory fashion. We have addressed the other in this patchwork process. So my question would be is it then possible to draft a uniform piece of legislation that would deal with the merchandising, marketing, collecting information arena

and avoid some of these conflicting statutory situations as one type industry moves and becomes a hybrid or a totally different industry all together and therefore transitions from one regulatory statute maybe to another. Is it reasonable or is it even desirable then that we attempt to consolidate this regulatory format into one uniform approach or is the patchwork quilt the better way to go and several of you have alluded to that and I don't care who responds.

Mr. FISCHER. Let me step out on that first—the first half of your question was are there other areas that are important and there are lots of them and the easiest place to see a summary of them actually is in the exceptions of Gramm-Leach-Bliley, for example, fraud control. The need to have the information to administer the account, government's access to information which is always a class of consumer desires and concerns. So you have all of those and you have lots of them out there.

Second, whether it's possible to come up with one single rule that governs all information I think it would be extremely difficult to do that just because the sensitivities, for example, that we've seen on health-related information is different than almost everything else. And so that alone would make a difference. To the extent that you would have to explain in any detail the one concern that I have about Gramm-Leach-Bliley, particularly, the size of the notice and whether consumers will actually be able to read them, if you were to do that, you would have to have a statement that was so short and so simple that no one could miss and you could apply it across lines. It would have to be something like we do have this information on you. We do provide to third parties for marketing purposes. If you don't want us to do that, please call the following number. Period. And so you could have something like that, but then you'd have to look at it, go through the same sort of cost benefit analysis we've talked about and say what benefits are no longer going to be there and at the end of that discussion you may well find that that's exactly what you want to do.

Mr. DEAL. Thank you.

Mr. STEARNS. Would you like any more response to your question?

Mr. DEAL. Are we going to have a second round?

Mr. STEARNS. I'm not sure yet. You asked your question. If there's any others that want to respond to that, I think that's fair.

Mr. DEAL. Yes, if anyone else would like to respond?

Ms. FORTNEY. I agree with what Rick has said and I think also part of your question dealt with the fact that if we had one comprehensive regulatory scheme that industries that are involved in multiple areas which are now regulated by different laws might find it easier to comply or it might make more sense in terms of uniformity. And I think that what we see today is that industries are very accustomed to working under many different statutes in many different areas, in both the Federal and the State level. And what they do is apply the laws or interpret the laws as they apply to those particular areas and the work that I do with clients, it does seem to function, I think it works much better than perhaps trying to have one piece of legislation that would fit all types of biosciences involved.

Mr. LAMB. I was just going to comment that the difficulty that we see with one size fits all is that the benefits of personalization and other aspects of information use vary so dramatically by product and service and industry that the cost benefit analysis may be different. And hen the tools that you have for implementing rules also very dramatically, from a computer in the Internet space, where communications is very easy, to the difficulties of dealing with somebody, for example, on a data service, on a hand-held wireless phone, where if you have one set of rules applying to both situations, the cost benefit might not work out in the same way in both places.

Mr. SMITH. I just want to comment really quickly on the issue of information use for marketing purposes. I think you can come up with some good general principles where you can cover a lot of different areas, but I just see the sensitivity of information is going to be a problem, that you need special cases for financial health, almost surely, but also on the qualitative and quantitative amount of information, on the Internet you get a lot of information about what people want, what articles they read and what they search for, this sort of thing, very, very details. It doesn't necessarily have to be personally identifiable. In the off-line world though everything is personally identifiable and you have very different kinds of information there that would probably require different rules or people would expect different rules.

Mr. STEARNS. The gentleman from Massachusetts, Mr. Markey.

Mr. MARKEY. Thank you, Mr. Chairman, very much. Thank you for having this very important hearing. As we all know, there is no omnibus privacy bill that has ever passed Congress. Instead, what we do is in each individual area try as best we can when an opportunity arises or a crisis arises, to pass legislation that adds to the privacy protection of Americans and that's why we have a Drivers' Protection Act, the Video Privacy Protection Act, the Fair Credit Reporting Act, the Privacy Rules in Gramm-Leach-Bliley, the On-Line Child Protection Privacy Protection Act for kids 12 and under, the laws against divulging information about which cable programs we are flipping to and fro and the Customer Proprietary Network Information where all of our telephone calls, who we're calling can't be divulged as well. So obviously over the years this Congress has looked at numerous areas that are in need of privacy protection. And I know that Mr. Smith has done great work in looking at the TiVo issue. One the one hand it can be advertised to each of us as a wonderful new service that allows us to watch any show we want any time we want without commercials, isn't that great? We're only thinking about you, in more ways than one, huh? So they can gather all this additional information about you as well, if they want, only with the promise that they won't divulge it.

Let me ask this, do you all agree that different types of information have different degrees of sensitivity, that health and financial data, TV viewing habits, web surfing data are more sensitive than other types of data such as a billing address? In other words, where my cell phone is billed to is less sensitive than where I call from and to whom I place calls, when and for how long I speak to whomever I might be talking to. Knowing that I subscribe to cable is less

sensitive than what shows I might be watching, especially later on at night. So do you all agree that there's a big distinction between those two categories of information?

Mr. LAMB. I would agree that consumers draw that distinction, but the distinction is different for each consumer, they make different choices. We have some consumers who, for example, in our case buy our $4.95 a month Internet access service which tracks, sends targeted ads to consumers and that's why we can offer it at that price and we disclose it very clearly to those consumers. Other consumers buy our more expensive service because they don't want to receive targeted ads, so they make that choice.

Mr. MARKEY. Right, so you work for AT&T, I know that.

Mr. LAMB. Yes.

Mr. MARKEY. But if I wanted you to give me Michael Armstrong's private telephone number you might not want to give that to me?

Mr. LAMB. I would say ask him.

Mr. MARKEY. I thought you would. Or if I ask you how much money you make, could you tell all of us because we could go online, maybe and find out if there weren't real privacy——

Mr. LAMB. Every consumer makes their choice.

Mr. MARKEY. That's what I'm saying is that almost all consumers are going to make the same choice you're making in those cases.

Mr. LAMB. Oh, I think in many cases, financial, medical, I agree.

Mr. MARKEY. That's the point I'm making. Yes?

Ms. FORTNEY. I agree that there are different sensitivities related to different types of information and also the detail that's involved in the information.

Mr. FISCHER. Agree.

Mr. MARKEY. Mr. Smith?

Mr. SMITH. Yes.

Mr. MARKEY. Do you think, Mr. Smith, it makes sense for us to have an omnibus privacy bill or should we do it piece by piece?

Mr. SMITH. Well, I think the golden rule is to where we start. I think a lot of privacy gets down to just expectations between people. I'm not sure that we can have an absolute omni bill. I think we can set aside some good principles in a bill, but back it up with specific bills that address specific areas.

Mr. MARKEY. Can each of you answer that question, please?

Mr. FISCHER. Yes sir, I'd be happy to. I do not think that you could have an omnibus bill. I think that given the variety of issues that we've talked about, the differences and sensitivity and the like, I think there really have to be differences and one of the things that I've discovered in my years of working this issue here is when the U.S. passes privacy laws, they expect them to be followed and they expect them to be enforced and that makes it really important. Europe might be a different approach where they pass the laws to feel good, but maybe not enforce them at all. Here, it is serious stuff and you really have to deal with them one at a time.

Mr. MARKEY. Let me ask one final question, Mr. Chairman, recently Mr. Dingell and Mr. Towns and I wrote a letter to the Federal Trade Commission requesting that the Federal Trade Commission analyze TiVo's services and data collection practices. We did that because the monitoring of the television viewing habits of

Americans is very serious business. And when people make their choices and their purchases, they should be aware of what the risks are that they're running.

Do you all agree that this is a serious issue, the TiVo issue in terms of their collection of data about Americans and that perhaps protections should be put on the books? Mr. Lamb?

Mr. LAMB. Absolutely. We don't have a relationship with TiVo, so I don't know what disclosures they made, but I absolutely agree with Mr. Smith that it is very important that you disclose to consumers what data you're collecting and it's only on that basis that consumers are going to be using these new products and services.

Mr. MARKEY. Thank you. Ms. Fortney?

Ms. FORTNEY. Let me just add to that. I agree that it is very serious, and also again I've not seen the TiVo disclosure, but based on Mr. Smith's description, I think it's important to recognize that if a company such a TiVo is using and disclosing information in a manner that's inconsistent with what it has told consumers and agreed to consumers that it would do, that would be a violation of Section 5 of the Federal Trade Commission Act which prohibits unfair deceptive acts or practices.

Mr. MARKEY. Okay, Mr. Fischer?

Mr. FISCHER. I think that if you have the delivery of an ad, as you do in a computer context, so that it is anonymous, but I'm still getting the benefit of the ad of something that I may be interested in given where I visited, it doesn't bother me.

If on the other hand as Mr. Smith said, there's information that's going to be tied to me by my identity, I would be very concerned.

Mr. MARKEY. So I want to congratulate you, Mr. Smith, on the excellent work which you've been doing on this issue.

Mr. SMITH. Thank you.

Mr. MARKEY. And Mr. Chairman, I would ask that my opening statement be placed in the record.

Mr. STEARNS. By unanimous consent, so ordered.

Mr. TOWNS. I'd like to have one thing cleared up, yes. I'd like to ask Mr. Smith——

Mr. STEARNS. By unanimous consent, 30 second.

Mr. TOWNS. All right. I'd like to ask Mr. Smith to clarify his response to my question regarding TiVo collection of home viewing information and home viewer serial numbers and let me quote from the Privacy Foundation Report, the reason I want to make certainly clear this up. It says, "however, the viewing information filed is nonetheless transmitted during a session identified by the home viewers' TiVo serial numbers. In fact, the serial number is transmitted multiple times during the single phone call. TiVo receives all of the information necessary to attribute the viewing information to a particular subscriber during this phone call, but gives no indication of this fact in any of its documentation. Therefore, the home viewing information can only be truly anonymous when TiVo Headquarters intentionally treats it as such. TiVo's current procedure does not change that fact."

Mr. SMITH. Okay, what's going on there, as we mentioned before, when the TiVo box phones the home, the first thing it does it get the program guide information. So it has to log in to the TiVo service to identify who the customer is, otherwise, people would get the

TiVo service for free. So that's why the ID number is sent in. In that same phone call, it also uploads this diagnostic log information which is giving some button presses and then in addition, it's sending up the viewing information and what they do is they make an effort to send that viewing information and deposit it in a way so that it's not tied directly to that ID number. That's a choice that they make at their servers, not in the box itself. So when we observed what was going on, all we saw was the data stream and we said there's no—they have to make that promise that they won't make that connection and after talking to them afterwards, that's what we learned. They said yes, we do not make that connection, but everything goes up in that same phone call. If these are computers talking, it's unlike human beings. They can kind of forget the first half of the conversation or the second half. Computers can do that. Human beings can't.

Mr. TOWNS. Mr. Chairman, I don't want to prolong this, but I'd like to get that answer in writing.

Mr. SMITH. Okay. From me?

Mr. TOWNS. Yes.

Mr. SMITH. Okay.

Mr. TOWNS. I don't want to prolong because I have some other parts. Thank you, Mr. Chairman.

Mr. STEARNS. The gentleman from Nebraska.

Mr. TERRY. Thank you, Mr. Chairman. Mr. Smith, real quick, once you opted-out, were you able to sniff and determine if they continued to keep track of programming?

Mr. SMITH. We haven't gotten that far yet. David Barton, who has the box just opted-out last week and went on vacation this week.

Mr. TERRY. Will you be doing that?

Mr. SMITH. Absolutely, but at the same time we trust TiVo to make that—if we do see something, I think it would be——

Mr. TERRY. Would you let us know if you find out?

Mr. SMITH. If it isn't, then there was a mistake made, I would say.

Mr. TERRY. I appreciate that. I was just curious. If there were any findings to that effect and obviously, I think, probably a key part of our discussion here or our conclusion is the legislative body is probably to create significant penalties when a violation, contract, whatever between the service and the customer is breached. I think that has to be a large component of whatever policy we adopt here.

Mr. Lamb, you seem to be left out of a lot of these questions, so I'm going to gear them toward you and then let it flow down the table.

I've reached the conclusion from everybody's testimony that it's going to be difficult to develop a comprehensive omnibus uniform whatever language you want to use. So it looks like we'll continue in a world of specific regulations for specific areas of which AT&T is showing us that in this world of technology today, many of those items overlap. They may be under the same umbrella. So you have to deal with the world of specialized privacy legislation. Can you describe in more detail how AT&T deals with overlapping and conflicting rules, what are the costs associated to it, do you develop a

different standard so you can try and comply to all of them at one time, set up separate silos? How do you deal with it and what are the costs?

Mr. LAMB. We do deal with it and the costs are substantial. What we end up doing is we have compliance with all the various statutory and rule structures and then across the company we have an overlay which is compliance with our own voluntary privacy policies on issues such as disclosure of personally identifiable data to third parties.

What happens though is that we have one account for a customer who might be buying wireless and cable and telephony for us in same cases, sometimes in a bundled price. So we have to flag data within that account and say this data can be used internally to market what we choose. This other data can only be used to market long distance, and this other data can only be used to market cable services, for example. So there is some probably artificial restrictions and query whether these internal restrictions really provide significant benefits to the consumers.

I know on issues such as disclosures to third parties, consumers have very real concerns. They want to know who has my data and what are they doing with it? We have not heard consumers telling us that they want to tie our hands internally to any great extent on what we do with their data, but in compliance with these statutes, we have to do exactly that.

Mr. TERRY. Do you think we can break it down? We may not be able to have a uniform policy on privacy that can cover both financial, medical, cable, broadcasts, telephony, wireless, all of that, but can we do it by industry, do you think? Do you think we could come up with one uniform policy that would enable AT&T to have one specific policy for wireless, telephone, cable?

Mr. LAMB. The difficulty is that industries aren't that clearly defined, at least in our experience and when they are, Internet versus telephony all of a sudden you cross Internet telephony and ask where that falls in the mix. So it is very difficult.

We do see the very high level principle of disclose what you're doing as being one that either is a result of self-regulation and voluntary actions or where necessary regulation and statutes, can be implemented. The details that we see in existing privacy statutes would not work and would have serious costs to have to try to apply the same set of rules across different technologies, but general concept of disclose what information you're collecting and what you're doing with it is one that we follow voluntarily and we don't think that really impedes anyone from doing business.

Mr. TERRY. Thank you.

Mr. STEARNS. Mr. Buyer?

Mr. BUYER. I always become a very good listener when I hear Mr. Deal give a Southern story. I know he's going to try to break down the complex and make it very simple and he made me reflect for a moment. I remember one of the first things of law school when we were discussing constitutional law and it was Justice Stewart said with regard to obscenity, "I know it when I see it." It's almost like privacy, it's so subjective, so when you gave your little rendition of the playground, that's what privacy is and each person's standard or belief of what privacy is is so subjective. What

one person thinks is private, another person doesn't really seem to care. We even learned you might come up to someone and actually touch them like this on the shoulder and say how are you doing and you didn't realize you've just offended them because you touched them.

Mr. DEAL. Yeah.

Mr. BUYER. Because I'm a damn Yankee, is that why?

Just haven't gotten over it yet.

But that's what I find in this. So Mr. Chairman, I really appreciate you having this hearing. It's one thing when we don't want to create more laws that are overlapping and make things more confusing and complicated and costly in implementation for you. However, I just want you to know from my perspective as we try to address these issues, sometimes we try to legislate in areas that's pretty difficult. I don't have a particular question for you, I just want to let you know that we're being very cautious as we approach this area. I don't believe that we really can—or the chairman asked you this question about sort of comprehensive approach. I don't think that you're going to be able to do that because every industry has its own unique set of problems and I don't know how we begin to measure harm. How do you do that? How do you decide—I just—I will elicit your comments because I don't know how we actually sit down to address this when, in fact, we want to give freedom. We want the Internet. We want the technology renaissance to continue, but how do we begin to address a society with one standard for harm when a lot of people care and some don't? I elicit your response.

Mr. FISCHER. Let me try that. If you look at Gramm-Leach-Bliley and you look at the notices that are out there and what people will be focusing on, you see paper. But ultimately what it's going to come down to is exactly what you said, what's the reaction going to be? So that frequently when I talk to people about what they're doing on information practices, what I saw is think about the family table, think about what it's like to tell everybody around the table what you intend to do with information and with whom and what do you think the reaction is going to be? If you feel good about that reaction around your table, then you probably are on safe ground. If you feel pretty queasy about it, then you shouldn't go there.

Mr. LAMB. I would just like to comment that we agree that privacy is a very subjective personal choice and I was recently asked how we balance the benefits of personalization against the loss of privacy and I said our basic approach is to try to let the consumer make that decision. We tell them what we're doing with a particular service and they tell us by buying the service or not, as long as we're very clear on our disclosure and with tools like P3P with which we've worked with Microsoft on that empower consumers to make their own privacy choices, I think that is the path that works best for us.

Mr. BUYER. Mr. Fischer, your answer to me, so when the Supreme Court Justice said "obscenity, I know it when I see it"—privacy, I know it when I feel it?

Mr. FISCHER. Yes sir, that's right.

Mr. BUYER. And that's what makes this so difficult. The one real plus about enforcement, it's very uncomfortable when you're there trying to advise somebody, but the real important thing about enforcement is when you see what happens to someone when they cross the line, you remember that, and you don't want to be there.

Mr. FISCHER. That's true.

Mr. BUYER. Ma'am?

Ms. FORTNEY. I would just like to add that I think a lot of the approach, what you're talking about here is really reflected in the approach of Gramm-Leach-Bliley which is for most information if you tell consumers what you're going to be doing and you give them the opportunity opt out. As in the case of Gramm-Leach-Bliley, that seems to be adequate. It really gets back to what Rick said and that is that if companies are uncomfortable telling consumers this is the information we have, this is how we're going to use the information, then that is going to have an effect on the ways in which they use the information. And then to set aside for more detailed and substantive regulation those areas which involve very sensitive financial, medical, similar types of information and to subject those to a different regulatory scheme.

Mr. BUYER. The great thing about notice, if I may, Mr. Chairman, is when people have this expectation of privacy, notice always begins to neutralized that.

Ms. FORTNEY. Right.

Mr. BUYER. Thank you. I yield back.

Mr. STEARNS. Mr. Smith, did you want to answer his question?

Mr. SMITH. Yes. I wanted to hit up real quick on the TiVo thing, our experience there. We got e-mail in on sort of both sides of the fence on that. Some people actually said we'd like TiVo to learn about our TV, what we watch on TV because we know this information is going to be passed on to the TV networks and our favorite shows won't get canceled then. So there clearly is even on something like this, there is multiple schools of thought. So we keep coming back to like a good notice on the TV set. They got the perfect device for doing notice and just a remote control to say yes or no. They have a good place to do it. Our concern was much more about how they did notice.

Mr. STEARNS. I thank Panel 1. We have a second panel here for members and we'd like to keep moving here, so we want to thank you very much for your time and your interest and we'll now move on to the second panel which is Ronald Plesser who is Partner, Piper, Marbury, Rudnick and Wolfe; Mr. Richard Varn, Chief Information Officer, State of Iowa; Mr. Frank Torres, Legislative Counsel, the Consumers Union; Mr. Jonathan Zuck, President, Association for Competitive Technology; and, Mr. Ed Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group.

I want to thank you for your patience and waiting and we'll start off, Mr. Plesser, with you with your opening statements I remind all the second panel that we would like them to keep it within 5 minutes. You're welcomed.

STATEMENTS OF RONALD L. PLESSER, PIPER, MARBURY, RUDNICK AND WOLFE; RICHARD VARN, CHIEF INFORMATION OFFICER, STATE OF IOWA; FRANK TORRES, LEGISLATIVE COUNSEL, CONSUMERS UNION; JONATHAN ZUCK, PRESIDENT, ASSOCIATION FOR COMPETITIVE TECHNOLOGY; AND EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR

Mr. PLESSER. Thank you very much and I very much appreciate attending and being asked to testify this afternoon. My name is Ron Plesser and I'm a Partner at Piper, Marbury, Rudnick and Wolfe and I was General Counsel of the United States Privacy and Protection Study Commission in the mid-1970's which was the last really organized omnibus, if you like, look at privacy laws and I've been asked today to talk about COPPA, the Children's On-Line Privacy Act. I'd also like to give a couple of overview observations and talk about the FTC Act, just slightly.

Let me start with the FTC Act. Anne Fortney mentioned it before and I think it is incredibly important as a privacy law and is often forgotten. It is clearly the basis that make self-regulatory efforts work. It is the basis, at least in part for the European acceptance of the safe harbor and what it does it prohibits deceptive and unfair statements.

A recent poll done by the FTC showed that I think over 80 percent of websites had some type of notice and what that means is that those notices, they don't have to be there, but once they're there, they have to be followed and they have to be enforced. The FTC has brought action in GeoCities, Liberty Financial and other cases where they have brought actions against people who have done something differently than they said and it is a very simple, but fairly potent piece of legislation.

COPPA is a very important piece of legislation and it has some flaws. I know several other people on the panel are going to discuss it. I'd like to just go through it fairly quickly and others can throw more detail on it. It does require notice. It does prohibit the collection of information from children without consent and I think the word collection is important. It's not just marketers collecting information. It's also facilitating the public accessibility of a kid's communication, chat rooms, postings, and these are areas that I think were consistent with some of the concerns that we have where we legislate where there is a problem. Clearly, in the chat room an don-line posting for kids 12 and under, there was problems. They were giving out home addresses. They were giving out information that at some level could harm them. This law meant to limit that. It also limited telemarketer collection of information. It's very important to note that it covered two situations, one where the website is aimed or directed at children and that's kind of a multiluck of the graphics, of the content, is this directed at kids? The second is where the site could be a general site, not directed at kids, but where they ask age and are informed that the kids register as being 12 or under. So those are the two circumstances. Verifiable consent is really the core of the restriction and hopefully I'll have a minute to give some observations about it.

One of the good things that the FTC did do is create a sliding scale in verifiable consent. They had a separate hearing on it in

July, I guess of 1999, where they found there was no real technology to allow verifiable consent on line, that the best you could do is kind of download a form, print and send and then fax it in with the parent's signature. So here was a law that required electronic verifiable consent, but yet, there was really no technology that permitted it and what the FTC did is created a sliding scale and did something very, very interesting. They've committed that they'll look at the issue again in April 2002 to determine if there's any new technology that will allow them to adjust the scale.

There are several exceptions for one time use in order to obtain the parent's consent for security purposes and with an opt-out for kind of subscription of repeated services and all of those cases the information can be retained, but it can only be retained for those purposes.

What are the important things about the COPPA that I think this committee could just use if I could just sum up. Couple of factors, one is technical flexibility. I think that's critical. The second is the roles of the Attorney General. It gave the Attorney Generals the right to enforce the Federal statute in Federal courts. As a result, we have seen very little State legislation developing on kids' privacy. We have a Federal standard with the Attorney Generals able to enforce it and the opt-in has worked the way I think most of us have thought, that it really has acted as a prohibition. The consumer, if it's not in 1 of the 4 exceptions, the chances are and I know Mr. Zuck will testify to this, that products and services have been discontinued. If a site knows that a kid's under 12, they just wire them out, take them out of the service. That's much easier than getting verifiable consent. I think it's a great example of opt-in.

The last issue that I would like to hopefully get back to in questions and answers is the defining issue of government access. We can do a lot in self-regulation, industry can do a lot. Programs like Carnivore, programs like the FBI collection of information, are difficult and I think if you look at most of the laws that we've enacted over the last 15 or 20 years, government access, the ability of government to demand those laws have been a defining part of it.

Thank you.

[The prepared statement of Richard L. Plesser follows:]

PREPARED STATEMENT OF RONALD L. PLESSER, PIPER MARBURY RUDNICK & WOLFE LLP

FEDERAL PRIVACY LAWS

The United States takes a sectoral approach to privacy regulation, adopting regulations only to deal with specific problems, subjecting some industries to extensive regulation and others to lighter or minimal regulation. This testimony will provide particular focus on regulation of children's privacy on the Internet and privacy regulation of electronic communications.

Since the 1970s, privacy regulation has generally been measured by five "fair information practice" elements articulated by the U.S. Privacy Protection Study Commission in 1977 and recently re-enunciated by the Federal Trade Commission. All federal privacy regulation encompasses at least two of the following features:

- **Notice** to the consumer regarding collection, use and disclosure to third parties of individually identifiable information obtained from him/her;
- **Consumer choice** either to opt out or opt in to use or disclosure to third parties of such information (in some cases disclosures to affiliates are subject to the choice requirement, in some cases they are exempt);

- **Access** to individually identifiable information collected about that particular consumer and an opportunity to **correct** inaccurate information;
- **Security** adequate to protect the information from unauthorized disclosure; and
- **Enforcement** of applicable privacy obligations.

A variety of other requirements—most often prohibitions against collection of information—apply in unique circumstances where a statute seeks to advance other policy goals. For example, the Children's Online Privacy Protection Act prohibits use of an activity to solicit from children more information than reasonably necessary to participate in the activity. Similarly, the Fair Housing Act prohibits collection of information used to engage in racial discrimination.

Finally, consumer protection law and the Federal Trade Commission Act offer a backdrop of limited protection even where no sector-specific privacy law applies. If a company posts a privacy policy, it can be held to its commitment to follow that policy under deceptive trade practice laws. Both the Federal Trade Commission and state attorneys general have begun bringing civil enforcement actions for deceptive trade practices against companies whose privacy practices have fallen short of their stated policies in a material way. Section 5 of the Federal Trade Commission Act gives the Commission authority in the context of commercial transactions to protect consumers against unfair and deceptive acts. This section 5 authority is what is the backbone of self-regulatory programs. While these programs, such as the Direct Marketing Association's privacy promise and the BBB *OnLine* program, are voluntary to begin with, they are thereafter enforceable if a company fails to do what it had said it would do. The FTC has proceeded against several Web sites that did not follow through on their commitments. This FTC authority is also the basis for the safe harbor program agreed to by the European Union and the Department of Commerce.

A. ELECTRONIC COMMUNICATIONS PRIVACY ACT

Congressional concern about technological advances in the years following enactment of the 1968 wiretap statute led to the enactment of the Electronic Communications Privacy Act of 1986 ("ECPA").[1] Through ECPA, Congress sought to extend the telephone network privacy safeguards codified in existing law to the new technology, including electronic mail and other computer-to-computer data transmissions. These communications are in many ways the electronic counterparts to letters, memoranda, or files transported via the postal system. ECPA addresses the problem of persons gaining unauthorized access—or exceeding their authorized access—to those electronic communications that, like personal or business correspondence, are intended to be kept confidential.

Specifically, ECPA's stored communications provisions[2] prohibit the unauthorized access to or use of stored electronic communications such as "voice mail" and electronic mail.[3] The exceptions to the rule of nondisclosure fall into three categories: (1) disclosures that are authorized by the sender or the receiver of the message; (2) disclosures that are necessary for the efficient operation of the communications system; and (3) disclosures to the government.

With regard to governmental requests for information, the Act usually requires that the customer be notified and given an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in the control of a provider of electronic communications services or remote computing services.

The law creates a civil cause of action against any party committing a "knowing or intentional" violation of these provisions.[4] The aggrieved party may seek injunctive relief and actual monetary damages (for amounts above the minimum award of $1,000) as well as attorneys' fees and costs.

---

[1] Pub. L. No. 99-508, 100 Stat. 1860.

[2] 18 U.S.C. §§ 2701 *et seq.*

[3] *Compare Steve Jackson Games, Inc. v. U.S. Secret Service,* 36 F.3d 457 (5th Cir. 1994) (in connection with e-mail, the offense of "accessing" covered by § 2701 governs the retrieval of communications *while in electronic storage* whereas the offense of "interception" covered by § 2511 governs the retrieval of communications while in progress), with *U.S. v. Smith,* 155 F.3d 1051 (9th Cir. 1998), *cert. denied* 119 S. Ct. 804 (1999) (in connection with voice mail, the offense of "accessing the facilities" is a lesser included offense of "intercepting the contents of the communication"; "intercept" entails actually acquiring the contents of the communication whereas "access" entails being in a position to acquire the contents of the communications).

[4] *See* 18 U.S.C. § 2707. But see, *Boehner v. McDermott,* 1998 WL 436897 (D.D.C. 1998) (federal legislator held to have a First Amendment right to publicly disclose content of illegally obtained cell phone conversation of Newt Gingrich).

B. IMPLEMENTATION OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998

In October 1999, the Federal Trade Commission completed its rulemaking implementing the Children's Online Privacy Protection Act of 1998 ("COPPA"). The FTC's Final Rule largely tracks the plain language of the statute, while providing additional detail on important issues such as who is covered by the Act, and acceptable forms of notice and of consent, among others.

The Rule went into effect on April 21, 2000, and online services and Web site operators who have actual knowledge that they are collecting personally identifiable information online from children or who target their Web sites or services or portions thereof to children under 13 years of age without complying with its requirements face the risk of prosecution by the FTC and State Attorneys General ("State AGs").

The Final Rule takes a practical and flexible approach to compliance with COPPA. Key elements include its application only *prospectively* to collection of personal information collected *online* from children, and adoption of a "sliding scale" approach to the statute's verifiable parental consent requirement, which allows the use of e-mail consent from a parent in certain circumstances for at least a two-year period. This "sliding scale" approach enables sites and online services to use an "e-mail-plus" mechanism for consent to internal uses of the data, while requiring sites and services to use print-and-send forms and other "more reliable methods of consent" for activities that allow children to provide information to third parties or that give children free e-mail accounts or chat room access.

1. Overview of the Rule

The statute and the Final Rule apply only to individually identifiable information collected online from a child ("personal information") by a Web site or online service that is targeted to children under 13 or that has actual knowledge that it is collecting personally identifiable information from a child under 13. Collecting information includes providing a child with the ability to have an e-mail account or the ability to post to a chat room, bulletin board or other online forum.

The Rule's primary goal is to require parental consent before a child can make personal information publicly available through chat rooms or e-mail. In addition, the Rule, subject to several exceptions, limits what information a commercial site can collect without prior parental consent even though there is no evidence of harm to children resulting from data collection from children.

It requires Web site operators and online service providers who engage in this form of online data collection to do the following:

a) Notice. Provide notice of their collection, use and disclosure practices;
b) Consent. As a general rule, obtain "verifiable parental consent" for the collection, use or disclosure of personal information subject to certain exceptions (some of which substitute a notice and opt-out requirement for consent);
c) Information Collected. Provide parents with a description of, and in some cases, the actual information that they have collected online from the child;
d) Opt Out. Allow parents to opt out of further use of the information;
e) Limit Collection. Avoid conditioning participation in an activity on disclosure of more information than reasonably necessary to participate; and
f) Security. Use reasonable data confidentiality, security and integrity procedures.

The FTC Rule lists acceptable means by which operators can obtain "verifiable parental consent." These means vary depending upon the intended use of the information. For internal uses of information, including marketing back to a child, Web sites may use e-mail consent accompanied by additional steps to provide assurances that the parent is providing the consent. These steps include sending a delayed confirmatory e-mail to the parent once the site has received the e-mail consent, or obtaining a postal address or telephone number from the parent and confirming consent by letter or telephone call.

By contrast, where a site offers chat rooms, message boards, or other similar features that enable children to make personal information collected online publicly available, or where the site discloses the information to third parties, it must obtain consent through sending back a printed form via postal mail or facsimile, the use of credit card numbers or toll-free phone numbers, digital signatures, or e-mails containing PINs or passwords obtained through any of these means.

Violators are subject to enforcement actions by the FTC or certain federal regulators with jurisdiction over particular industries and by State AGs. Web sites and online services may comply with the Rule either by following the Rule in its entirety or by following self-regulatory guidelines approved by the FTC.

2. Who Is Covered by the Final Rule's Obligations?

a. Commercial Sites and Online Services—The Final Rule exempts all non-commercial sites and online services. This is consistent with FTC authority, which extends only to commercial activities. Nonprofit status alone may not exempt prohibited practices. The Rule does not define specifically the line between commercial and non-commercial sites, and whether a nonprofit engaged in commercial activity would be subject to the Rule.

b. "Directed to Children"—The Final Rule applies to all Web sites and online services, or portions of sites and online services that are targeted to children under the age of 13 within the meaning of 312.2 of the Rule. This is a flexible inquiry that involves assessment of "the overall character of the site," including whether:

- there is child-oriented content on the site, which includes an assessment of the age of models on the site, presence of animated characters, children's music, and/or child-oriented activities and incentives (such as puzzles, games, or trivia);
- the ads appear to be targeted at children under 13;
- the language is targeted toward an audience under 13;
- there is reliable empirical evidence regarding the age of the site's visitors; and
- there is evidence regarding the intended audience.

The Rule does not look only to whether a site or service is targeted to children *in its entirety*. If a portion of a site or service (such as a child-oriented pen pal service) is targeted to children, then the requirements of the Final Rule will apply to that portion only. Merely referring or linking users to a site that is targeted to children does not subject an operator to the Rule, and linking to a site that violates the Rule creates no liability. However, if other elements of a site indicate that the site is a child-oriented directory, then it would be considered targeted to children under the Rule.

Web sites and services that are targeted to children and that have not obtained prior parental consent will be required to monitor their chat rooms, message boards and similar services and delete individually identifiable information that children post about themselves.

c. Not "Directed to Children"—The great majority of operators of general audience sites and online services that do not target their offerings to children are regulated under the Rule only if they have actual knowledge that they are collecting information online from a child. Sites and services that ask the age of visitors are therefore subject to the Rule's requirements if they allow respondents who indicate that they are under 13 onto the site or service. In addition, the Final Rule indicates that receiving information "from a concerned parent who has learned that his child is participating at the site" gives the site actual knowledge. It does not indicate whether notice from third parties provides such knowledge.

The commentary on the Rule indicates that the FTC will "closely examine" sites that appear to be determining through "age-identifying questions" whether a visitor is a child "without specifically asking for the visitor's age" to determine whether these sites in fact have actual knowledge. For example, asking whether a visitor attends elementary school may give a site actual knowledge that it is collecting information from children. Similarly, the FTC "will look closely at" sites that ask for age ranges that include both children and teens (*e.g.*, "15 and under") to determine whether they "are trying to avoid compliance with the Rule."

d. Collecting Information Online from Children—The Rule defines the act of collection as any means "enabling children to make personal information publicly available through a chat room, message board, or other means, *except where* the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records."

This means that if an operator obtains actual knowledge that it has collected personally identifiable information online from a child, it may either comply with the substantive requirements of the Rule or delete the information from its own records before it is made public.

Therefore, online fora (such as chat rooms, message boards and similar services) targeted to children that do not obtain prior parental consent will need to put in place a process for: (1) moderating and monitoring "real time" postings by children; (2) delaying making postings containing personal information publicly available until such information has been stripped from them; and (3) deleting that information promptly from the operator's records.

Similarly, sites and services that are not targeted to children under 13 years of age, but that obtain "actual knowledge" that a posting contains personal information

disclosed by a child may redact it of personal information both at the site and in their own databases as an alternative to complying with the Rule's requirements.

e. Responsibilities of Intermediaries and Third Parties Who Receive Personal Information—Often information collected at an online site passes through several entities who could be deemed to collect the information—for example, the Web site host, Web site content provider and its affiliates, and advertisers on the site. The Rule adopts a case-by-case, functional approach to determining what entity in these situations is actually subject to the Rule, examining ownership and control of the information, payment for and contractual arrangements for collection and maintenance, and whether the site "is merely a conduit through which the information flows to another entity."

Internet access providers who do not target children or have actual knowledge that they are collecting personal information from children are exempt from the Rule. In addition, third parties that receive information from operators are exempt from the Rule's requirements, although they may find that operators often restrict by contract their ability to use the information or disclose it to others.

3. The Rule's Requirements

Operators that are covered by the Rule, must comply with the Rule's five principal functional requirements: (1) providing notice, (2) obtaining prior parental consent in most circumstances or complying with notice and opt out in most other circumstances, (3) affording parents access to personal information collected online from their child and the opportunity to opt out of further maintenance and use of that information, (4) following the Rule's security requirements, and (5) avoiding conditioning participation in an activity on disclosure of more personal information than reasonably necessary to participate in the activity.

a. Notices—Operators must provide notice, both on their Web site at each point of collection and directly to parents in circumstances where parental consent or notice and opt out are required, of their collection, use and disclosure of personal information. The FTC's Final Rule prescribes in considerable detail the content of the privacy notice that operators must provide on their Web site and directly to members. The notice:

1) Must be located on the operator's home page and accessible at all data collection points;
2) When provided directly to parents as discussed in section b below, must be provided via e-mail or as part of a print-and-send form where the site or service is subject to consent or notice and opt out.
3) Must be labeled specifically as a notice of the site's information practices regarding children;
4) Must disclose, directly or through the operator of another site (whose name, address, phone number and e-mail address must be listed at the original operator's site), the name, address, phone number and e-mail address of third-party collectors of information at the site, the types of personally identifiable information collected and whether information is collected directly or passively;
5) Must disclose whether third-party contractors have agreed to maintain confidentiality, security and integrity of information;
6) Must disclose how the information will be used (including fulfillment of a transaction, record keeping, marketing or public disclosure) and the types of businesses to whom the information may be disclosed;
7) Must list parents' rights under COPPA and procedures for providing consent and obtaining access to their children's information;
8) Must disclose that the site or online service may not condition a child's participation in an activity on the disclosure of more personal information than reasonably necessary to participate in the activity.

b. Verifiable Parental Consent and Notice and Opt-out Requirement—**1. Parental Consent Requirement and Sunset for E-mail Consent—**As a general rule, operators should obtain informed parental consent before the collection, use and disclosure of personal information collected online from a child.

In the case of personal information that is part of *public postings or disclosed to third parties,* consent must be obtained through print-and-send forms via postal mail or facsimile, the use of credit card numbers or toll-free phone numbers, digital signatures, or e-mails containing PINs or passwords obtained through any of these means. These consent methods must be used for "activities involving chat rooms, message boards, disclosures to third parties, and other 'disclosures.'"

In the case of personal information that the operator makes only internal use of, consent may be obtained through any of the above means. At least until April 2002, consent may also be obtained for these purposes through e-mail accompanied by "additional steps ...to provide assurances that the parent is providing the consent."

These include "sending a delayed confirmatory e-mail to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming consent by letter or telephone call." The Commission will "phase out" the sliding scale in April 2002 "unless presented with evidence showing that the expected progress in available technology has not occurred." The Commission intends to begin a notice and comment period with regard to this sunset in October 2001.

Operators must offer the parent the option of consenting to collection and internal use of personal information collected from the child without consenting to disclosure of the information to third parties. However, release of personal information to a person who uses the information solely to provide support for the internal operations of the Web site or service, including technical support and order fulfillment, is not considered a "disclosure," and parents may not prevent these disclosures if they agree to collection and use of the information.

2. Notice and Opt Out—Operators may provide direct parental notice and the opportunity to opt out of further retention of the information, instead of parental consent, in two circumstances:

The first is for collection of a child's e-mail address for the sole purpose of responding more than once to a specific request of a child (such as subscription to an online newsletter, contest entry, or customer service request) where the e-mail address is not used for any other purpose. This exception is framed quite broadly and may be useful to operators in a significant range of circumstances.

The second is for a limited child safety exception which permits an operator to collect a child's name and online contact information to the extent reasonably necessary to protect the safety of a child user (*e.g.,* to report evidence of child abuse) where the information is used only for that purpose, not used to recontact the child for any other purpose, and not disclosed on the site or service.

3. Exceptions to Consent and Notice and Opt Out—Operators may collect personal information without either obtaining parental consent or providing parental notice and an opportunity to opt out in the following circumstances:

- For collection of a child's e-mail address for the sole purpose of *responding on a one-time basis to a specific request of a child,* after which the address is deleted;
- For collection of the child's or parent's name and online contact information for the sole purpose of *obtaining parental consent or providing notice of a parent's right to opt out*, if the information is deleted within a reasonable time after the date it is collected;
- In a school-based setting in which the operator provides notice of its collection, use and disclosure practices to the school and the school provides consent *in loco parentis* (the Commission also intends to issue guidance to the educational community regarding the Rule's privacy protections); or
- To the extent reasonably necessary to protect the security or integrity of the site or online service (*e.g.*, to prevent hacking), to take precautions against liability, to respond to judicial process, or to the extent consistent with other provisions of law, to provide information to law enforcement or for an investigation related to public safety, provided that the information is not used for other purposes.

c. Access and Opt-out Requirements—Operators are required to provide parents with access to the types of personal information collected online from children, and with "a means that is reasonable under the circumstances" for the parent to obtain the specific personal information the operators have collected. Before providing access to the actual information collected, operators must make efforts to verify that the requester is in fact the child's parent. These efforts include not only secure procedures such as password protected e-mail, but any acceptable method for obtaining parental consent to third-party disclosures, discussed above. The Rule indicates that operators who follow one of these procedures acting in good faith to a request for parental access are protected from liability under federal and state law.

The access requirement does not apply to information collected from offline sources or collected before the effective date of the Rule unless it cannot be distinguished from personal information covered by the Rule. In this instance, operators may be required to provide access to compilations of personal information merged or enhanced with other information.

Operators must also afford parents the opportunity to have personal information collected from their child deleted from the operators' databases and to have the operator cease using or collecting the information. This opt out simply revokes consent that the parent has previously provided. It does not prevent the operator from seeking and obtaining parental consent in the future.

d. Security Requirement—Web sites and online services that are covered by the Rule must establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information. The Commentary to the Rule indicates that such procedures include secure Web servers and firewalls, deleting in-

formation once it is no longer used, limiting employee access to data, providing data-handling training to employees who do have such access, and careful screening of third parties to whom the information is disclosed. Noting that security measures can be costly, the Commentary gives operators discretion "to choose from a number of appropriate methods of implementing this provision."

e. Limiting Collection—The Rule also places some limits on the collection of personal information by covered Web sites and online services. These operators are prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than reasonably necessary to participate in the activity. This measure is designed to prohibit tying a child's ability to participate in a prize or game to disclosure of personal information that is not necessary for the activity in question.

4. Methods of Complying

a. Safe Harbor—COPPA allows operators to comply by following self-regulatory guidelines approved by the Commission after notice and comment.

The Rule provides that to qualify for the safe harbor, self-regulatory guidelines need not be identical to the Rule, but must have "substantially similar requirements that provide the same or greater protection." Guidelines must include an effective, mandatory mechanism for independent assessments of operators' compliance with the guidelines through periodic reviews or any other equally effective mechanism. They must also include an effective incentive for compliance by operators who commit to follow the guidelines, including mandatory public reporting of disciplinary actions taken against operators who violate the guidelines, referrals to the FTC of operators who engage in a pattern and practice of violations, consumer redress, voluntary payments to the U.S. Treasury, or any other equally effective incentive.

Self-regulatory organizations who obtain safe harbor treatment must retain for at least three years and make available to the FTC upon request all consumer complaints alleging violations of the guidelines, records of disciplinary actions taken, and the results of the independent assessments that are part of the self-regulatory program.

b. Enforcement—The FTC will monitor the Internet for compliance with the Rule and bring law enforcement actions to deter violations where appropriate. Violations of the Rule are trade regulation violations and subject the violator to civil penalties of up to $11,000 per day for each violation. The FTC also has authority under Section 5 of the FTC Act to sue to obtain a final cease and desist order, temporary restraining orders with or without notice, restitution, disgorgement of profits, and other equitable relief.

COPPA also provides states and other federal agencies with authority to enforce compliance with the Rule. State AGs can bring suit on behalf of citizens in their state to obtain appropriate relief including enjoining the practice, enforcing compliance, or obtaining compensation on behalf of residents of their state. A series of federal agencies that have jurisdiction over regulated industries receive enforcement authority over violations of the Rule by those industries. For example, the Office of the Comptroller of the Currency has authority over national banks, and the Department of Transportation has authority over air carriers.

OVERVIEW OF FEDERAL PRIVACY LAWS

Following is a brief description of laws adopted by Congress in response to the privacy issue.

A. INTERNET PRIVACY

1. Children's Online Privacy Protection Act (15 U.S.C. §§ 6501 et seq.)

This statute, adopted by Congress in 1998, is the only federal law that specifically regulates Internet privacy. It applies only to web sites and online services, and agents of web sites and online services, who have actual knowledge that they are collecting information from children under 13 (for example, by asking age), or who target a portion of their site or service to children under 13.

COPPA requires these sites and services ("operators") to post a **notice** of their privacy practices on the web site; to obtain verifiable **parental consent** for collection, use, or disclosure of a child's personally identifiable information; to provide parents with the opportunity to **access** the information collected from their children, as well as to have the information corrected or deleted from the company's databases; and to maintain data **security** and integrity procedures. Violations are **enforceable** by the FTC and state attorneys general as unfair and deceptive trade practices. Companies and trade associations may seek approval of self-regulatory

guidelines that meet all the requirements of the law and the FTC's implementing rules. COPPA preempts inconsistent state laws.

B. PRIVACY IN OTHER COMMUNICATIONS MEDIA

1. Cable Privacy—Cable Communications Policy Act (47 U.S.C. § 551)

This act requires cable television operators to provide **notice** to their subscribers annually and at the time of initiating service about the nature of personal data collected, data use and disclosure practices, and subscriber rights under the statute. Prohibits a cable television company from **collecting** individually identifiable information about its subscribers over the cable system without their **prior written consent.** Generally bars cable operators from **disclosing** such data without **prior written consent,** except for disclosure of lists of subscriber names and addresses that do not reflect subscriber viewing habits or transactions over the cable system. Requires subscriber **access** to all personally identifiable information regarding the subscriber and a right to correct any errors. Enforcement is through a private right of action. Requires **destruction** of individually identifiable information when no longer necessary for the purpose for which it is was collected. Authorizes damage awards of $100 per day and at least $1,000 per violation, as well as awards of punitive damages, costs, and attorneys' fees against cable television companies that violate the Act's subscriber privacy provisions. Several multi-million dollar class action lawsuits have been filed under this statute.

Also prohibits a cable operator from providing personal subscriber data in its possession to a governmental entity absent a court order reflecting a judicial finding of clear and convincing evidence that the data subject is reasonably suspected of criminal activity and that the information sought would be material. Subscribers must be notified and provided with an opportunity to contest the government's claims.

The Administration recently proposed lowering this standard to reconcile it with access to subscriber information under the wiretap statute, which requires a lesser showing of suspicion of criminal activity and does not require notice to the subscriber.

2. Telecommunications Privacy—Customer Proprietary Network Information (47 U.S.C. § 222)

Applies to data obtained by a telecommunications carrier concerning a subscriber's subscription to and use of telecommunications service (not Internet services). However, does not apply to subscriber name, address and phone number. Restricts private sector **use or disclosure** to third parties of this individually identifiable customer data without prior **customer approval,** except to provide services to which the customer has already subscribed. Requires telecommunications carriers to protect the **confidentiality** of the data, including restricting internal access to the information. Enforcement by the FCC.

Telephone subscription and usage information is a significant competitive asset, and the statute has a second purpose of helping to advance telecommunications competition. Therefore, it applies not only to *consumer* data, but also to data of telecommunications companies and equipment manufacturers. It also *requires* disclosure of customer data to competitors at the customer's request, and prevents local telephone companies from using aggregate customer data unless they provide competitors with non-discriminatory access to those data.

3. Telephone Consumer Protection Act (47 U.S.C. § 227)

Requires entities that use the telephone to solicit individuals to provide such individuals with the ability to **opt out** of future telephone solicitations. Requires entities that engage in telephone solicitations to maintain and honor lists of individuals who request not to receive such solicitations for 10 years. **Prohibits** unsolicited commercial telephone calls using an artificial or prerecorded voice without consumer consent. **Prohibits** the sending of unsolicited advertisements to facsimile machines.

4. Electronic Communications Privacy Act (18 U.S.C. §§ 2701 et seq.)

Prohibits persons from tampering with computers or accessing certain computerized records without authorization. The Act also prohibits providers of electronic communications services from disclosing the contents of stored communications. Usually requires that the customer be notified and given an opportunity to contest in court a government entity's request for access to electronic mail or other stored communications in the control of a provider of electronic communications services or remote computing services.

5. Wiretap Statutes (18 U.S.C. §§ 2510 et seq.; 47 U.S.C. § 605)

Prohibit providers of electronic communications services from disclosing the contents of electronic mail, radio communications, data transmission and telephone calls without consent or a court order. The Federal Communications Commission also has a rule and tariff prescription prohibiting the recording of telephone conversations without notice or consent. *See* 47 C.F.R. § 64.501; 5 FCC Rcd 502 (1987).

C. OTHER ENTERTAINMENT

1. Video Privacy Protection Act (18 U.S.C. § 2710)

Affords users and purchasers of commercial videotapes rights similar to those of patrons of libraries. Prohibits videotape sale or rental companies from disclosing customer names and addresses and the subject matter of their purchases or rentals for direct marketing use, unless they provide customers with **notice** and the opportunity to **opt out** of such disclosures. Disclosure is also permitted with the customer's consent or court approval. Requires that subscribers be notified and provided with an opportunity to contest a data request prior to a judicial determination. **Enforcement** is through a private right of action. Video companies that violate the Video Privacy Protection Act may be liable for damage awards of at least $2,500, punitive damages, costs, and attorneys' fees.

D. FINANCIAL PRIVACY

1. Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 et seq.)

Regulates the privacy of personally identifiable, nonpublic financial information disclosed to non-affiliated third parties by financial institutions. Requirements also attach to non-affiliated third parties to which they transfer this information. Requires written or electronic **notice** of the categories of nonpublic personal information collected, categories of people to whom the information will be disclosed, consumer opt-out rights, and the company's confidentiality and security policies. Creates consumer right to **opt out** of disclosures to *nonaffiliated* parties before the disclosure occurs, subject to a long list of exceptions. Requires administrative, technical and physical safeguards to maintain the **security,** confidentiality and integrity of the information. Prohibits disclosure of account numbers and access codes for credit, deposit or transaction accounts to a nonaffiliated party for marketing purposes except to a consumer reporting agency subject to the Fair Credit Reporting Act. Enforcement is by the FTC or applicable banking or securities regulators.

The notice and opt-out requirements do not apply unless an institution or one of its affiliates discloses the information to a nonaffiliated third party. However, once those requirements take effect, the institution must provide notice of its practices with regard to disclosures to *both* affiliates and nonaffiliated parties.

The requirements apply directly to both financial institutions and the nonaffiliated third parties to which they disclose nonpublic information. Unless it complies with these requirements, a nonaffiliated third party that receives nonpublic information from a financial institution is prohibited from disclosing such information to anyone who is not affiliated with both the receiving third party and the financial institution.

2. Fair Credit Reporting Act (15 U.S.C. §§ 1681 et seq.)

Regulates the collection and use of personal data by credit reporting agencies. Requires that when a data broker is hired to prepare an "investigative consumer report" (an investigation into the consumer's "character, general reputation, personal characteristics, or mode of living" by means of interviews with friends, neighbors, and associates), the request for information must be disclosed to the subject of the report, who is then entitled to learn the nature and scope of the inquiry requested. Requires that, if a consumer report is used in any decision to deny credit, insurance, or employment, the report user must tell the consumer the name and address of the reporting agency.

Requires credit reporting agencies to provide **notice** to consumers of their rights whenever a consumer requests access to the contents of the consumer's file. Prohibits disclosure of consumer reports maintained by consumer reporting agencies without **consent** unless such disclosure is made for a legitimate business purpose or pursuant to a court order. Requires consumer access to all information in the consumer's file, right to challenge accuracy of information in the file, and right of reinvestigation when a consumer disputes the accuracy of information in his or her file. Requires brokers to maintain **security** procedures, including procedures to verify the identity and stated purposes of recipients of consumer reports. 15 U.S.C. §§ 1681 *et seq.*

Enforcement is through a combination of private lawsuits, agency enforcement and criminal penalties. Creates private right of action against credit reporting agencies who disclose or parties who obtain consumer reports in violation of the Act. Individuals may recover for actual damages suffered, as well as attorneys' fees and court costs. Punitive damages or criminal penalties may also be imposed for willful violations of the Act. The Federal Trade Commission and other federal agencies responsible for enforcing the provisions of this Act also are empowered to declare actions to be in violation of the applicable statute, issue cease and desist orders, and impose statutory penalties for noncompliance with agency orders.

Requires reporting agencies to use procedures that will avoid reporting specified categories of obsolete information and to verify the accuracy of information in investigative consumer reports that are used more than once.

3. Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)

Requires banks to make extensive disclosures to customers about specific electronic funds transfer (EFT) transactions, both at the time the transactions are made and in the form of periodic statements. Requires banks to provide **notice** to customers, at the time they contract for EFT services, of their rights, liabilities, charges, procedures, etc., connected with the services, and of whom to contact if an unauthorized transfer is suspected. In the case of pre-authorized periodic transfers—such as automatic bill paying—the bank must provide either positive or negative notice as to whether payments are being made on schedule. Mandates detailed procedures for the resolution of any inaccuracies in customer accounts, and imposes liability on the bank for errors in the transmission or documentation of transfers. **Enforcement** is through a combination of private lawsuits, criminal penalties and regulatory enforcement. An individual who prevails in a civil action for a violation of the Act may recover actual damages sustained, a penalty of $100 to $1,000, attorneys' fees and court costs, and in limited situations, treble damages. Criminal penalties may be imposed for deliberate violations of the Act. Numerous federal agencies also have administrative responsibility for enforcing the provisions of this Act.

4. Equal Credit Opportunity Act (15 U.S.C. §§ 1691 et seq.)

Restricts inquiries into a credit applicant's sex, race, color, religion, or marital status. Prohibits the retention and preservation of certain information by creditors and requires the preservation of certain specified records relating to credit transactions. Regulates the manner in which information collected by creditors may be used in making decisions regarding the extension of credit. Requires that, when credit is denied or revoked, the applicant must receive **notice** either of the reasons for the decision or of his right to learn the reasons. **Enforcement** is through private lawsuits and administrative enforcement. Private plaintiffs may recover actual damages, punitive damages, attorneys' fees, and court costs. Individual or class action suits may be maintained for administrative, injunctive, or declaratory relief. Numerous Federal agencies also have enforcement responsibility for the provisions of this Act.

E. MEDICAL PRIVACY

1. Health Insurance Portability and Accountability Act and Regulations (Pub. Law No. 104-191 §§ 262, 264; 45 C.F.R. §§ 160-164)

The Health Insurance Portability and Accountability Act of 1996 gave the Department of Health and Human Services ("HHS") authority to adopt privacy regulations if Congress failed to legislate in this area by December 31, 1999. On December 28, 2000, HHS released a highly regulatory final rule for implementing these privacy provisions, which goes into effect on February 26, 2003 and will be enforced by HHS's Office for Civil Rights.

Requires health plans and health care providers to provide a written notice of how protected health information about an individual will be used, as well as an accounting of the circumstances surrounding certain disclosures of the information. Prohibits plans and providers from disclosing covered information in a manner inconsistent with the notice.

Requires covered entities to obtain a patient's **opt-in** via a "consent" form for both use and disclosure of protected information for treatment, payment or health care operations. Also requires covered entities to obtain a patient's more detailed **opt-in** via an "authorization" form for both use and disclosure of protected information for purposes other than treatment, payment or health care operations.

Permits several forms of marketing and fundraising uses of protected information subject to receipt of written consent. Requires separate patient authorization for transfers of protected information for routine marketing by third parties. Provides right to **access,** copy, and amend the information in designated record sets, including in a business associate's records if not a duplicate of the information held by

the provider or plan. HHS would enforce the rules through a variety of sanctions, including denying federal funds to violators.

Applies to individually identifiable health information that has been maintained or transmitted by a covered entity. Will apply directly to three types of entities: (a) health plans, (b) health care clearinghouses, and (c) health care providers. Also will require these covered entities to apply many of its provisions to their business associates, including contractors, third-party administrators, researchers, life insurance issuers, and employers.

F. STUDENT PRIVACY

1. Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)

Requires schools receiving public funds to provide **notice** to parents of minor students, or students over 18 years of age of their rights under the statute. Prohibits schools from using or disclosing individually identifiable contents of a student's records without the **consent** of the student or of the parent of a minor student. Provides exemptions from consent for disclosures for a variety of educational, statistical, and public safety purposes. Allows disclosure of data-specific items including name, address, telephone number, date and place of birth, major, sports participation, dates of attendance, and degrees and awards received, if the school provides public **notice** of its disclosure policy and the opportunity to **opt out** of disclosures.

Permits a student or the parent of a minor student to obtain access to and a hearing to challenge the accuracy or completeness of educational records that concern the student. Vests administrative enforcement of the Act in the Department of Education, and provides for termination of Federal funds if an institution violates the Act and compliance cannot be secured voluntarily.

Prohibits government access to personal data in educational records without a court order or lawfully issued subpoena, unless the government is seeking access to the records for a specified education-related purpose.

G. CIVIL RIGHTS AND POLYGRAPH PRIVACY

1. Fair Housing Act (42 U.S.C. §§ 3604, 3605)

Restricts the collection and use of information that would result in housing discrimination on the basis of race, sex, religion, national origin and a variety of other factors.

2. Equal Employment Opportunity Act (42 U.S.C. §§ 2000e et seq.)

Restricts collection and use of information that would result in employment discrimination on the basis of race, sex, religion, national origin, and a variety of other characteristics. 42 U.S.C. § 2000e, *et seq*.

3. Employee Polygraph Protection Act (29 U.S.C. §§ 2001 et seq.)

Prohibits employers from requiring a polygraph test as a condition of employment or using the results of such tests as the sole basis for disciplining employees or taking other adverse employment actions. Bars employers from publicly disclosing the results of polygraph tests unless disclosure is made to the government pursuant to a court order or for the purpose of providing the government with information on criminal conduct. Employers that violate the Act may be subject to a fine of up to $10,000, injunctive relief such as employee reinstatements, and awards of damages, costs, and attorneys' fees.

Mr. STEARNS. I thank the gentleman.

Mr. Varn.

STATEMENT OF RICHARD VARN

Mr. VARN. Thank you, Mr. Chairman. I've been involved with this issue also for about 25 years, chairing the Information Technology Policy Task Force of NCSL, National Conference of State Legislatures for 3 years, got them to create a committee, a standing committee to deal with this and was involved and currently chair NAISR which is people like me, CIOs of the state. They're a group on privacy and personalization of information.

Provided to you also in your attachments to this material, a guide to help policymakers like yourself deal with these difficult issues and try to balance these and I'd commend it to you. It's a

short read and it was designed with people—written for people like you.

I certainly appreciate the deliberative approach you're taking here, the approach I think is warranted for these reasons. Information is a natural resource to the modern economy in a democracy and technological environment information is, in fact, the fuel of our future. We've learned from experiences like Y2K and the energy shortages we've experienced, that these systems are interconnected in ways that are very complex and we depend on them. Changes in one part tend to trigger changes, unattended consequences ripple throughout the economy in ways we can't even imagine since they're so tightly interconnected.

In fact, the flow of information has become as vital as the flow of energy in our world, neither the benefits of this information flow nor the cost of its restrictions are fully apparent or even known, making this deliberative approach necessary and some watchful waiting advisable.

To that end, I want to cover a few issues related to DPPA, a little bit to voter registration and specifically what local government and states are doing to relate to this issue and cover the rest in questions.

Specifically, I want you to think of these things as four separate issues because to do otherwise leads to confusion in almost all discussions, when I was a lawmaker for 12 years and since I've been in the administrative branch. Split it into these talks. Privacy, the who, what, when, where, why and how of policies and date where our values are expressed as another congressman talked about, where our values are expressed and then codify it to the extent we can; security, where we actually enforce those privacy policies; integrity, where we guard against the accidental or purposeful changing or loss of our information; and finally, accuracy, the quality assurance and customer-friendly processes that lets people find and correct information errors in government records.

With those four areas in mind, I've also provided a list to my testimony of other sort of methodical approach to trying to solve these problems. I hope the categories I have provided you allow you to target your solutions more accurately to the problems of bad actors or whoever is causing the problem and I encourage you also to consider some proactive measures. For example, our identify system is fundamentally broken. I'll talk a little bit more about that in a second. Consider also investment in law enforcement teams to go directly after identity theft and also services such as consider an identity theft advocate being something in an Attorney General's office or elsewhere that would help people repair their good reputation and their good credit.

As we've noticed in the DPPA, the acts rely on trying to keep common facts like your address secret and that is then—becomes this very weak and unreliable security method. It's supposed to be the firewall between you and evil. It can't work that way. Common facts are out of the bottle and they can't be put back in, things like address can't protect you from violence. Especially in that case, the very person, the private detective who actually found the information that led to the incident of killing the actress ended up being

exempted, the very private detective that could have found it, could find the information after the law passed in the DPPA.

I also note that voter registration, while it was well intended, the Motor Voter Act, as you encourage people to register to vote, I'd also note that underlying all that is an antiquated system of voter registration, that you do need to help us invest in and to change. Some matching grants from Congress will help legislators focus on that issue because it isn't so much in getting people to vote, it's actually having these systems work and talk to each other and I don't think that the issue there is privacy. I think you all want access to that type of information so our democracy will work.

Local governments are just not keeping up in many cases. It's a patchwork. They are a drag on our privacy, security, access and e-government issues and we need to find ways to encourage them to establish and maybe just some voluntary guidelines to encourage them to bring those up. And why do I bring that? The very fact of civic and economic citizenship for Americans is established and extinguished by the birth, marriage and death records created at the State and local level. You all build off of those to create Social Security numbers and passports and we chime in to having actual driver's licenses and voter registration. This bedrock is a shaky one. It is not founded on things that are sound. Note this, if paper birth certificates, Social Security number, your mother's maiden name, your city of birth, your name and address are these crumbling pillars of identity, all of these things are easily stolen and forged and this is not going to get back in the bottle soon either. These facts and these paper systems are not going to work. These components of identity worked when everybody knew each other. This doesn't work any more. Many states, such as mine, are moving forward with things like public key encryption and also with digital signatures and biometrics to be able to allow our citizens choices to strengthen their identity. Things like DPPA that tried to keep simple facts away from people are not going to work in a modern era of modern commerce where we do business with people we never see or know.

Finally, as we are engaged in a lot of these activities, I would say that states are a good laboratory for you to follow. I would note that in Congress and as with State legislators, to conclude, anecdotes are the catalysts for legislative policy. Stories tell it best to us.

I'd also remind you that hard cases make very bad law and in the states we most have CIOs, there's no Federal CIO yet. There's no one committee of Congress who focuses on information policy. No wonder it's a patchwork. We haven't stacked up in each branch of government people to deal with these policy areas. Too much time and effects and not enough time, I think, on the bad actors.

In conclusion, don't forget, there are many government functions that require personalization and use of every bit of information we collect to enforce the laws you pass on down to the states. So in order to be able to catch the person who is delinquent in their child support, we must relate various bits of information to other bits. The same thing happens in the private sector, to deliver good customer service.

Thank you.

[The prepared statement of Richard Varn follows:]

PREPARED STATEMENT OF RICHARD VARN, CIO, STATE OF IOWA

WHY A DELIBERATIVE APPROACH IS WARRANTED IN THIS AREA

Information is like a natural resource to a modern economy and democracy. Information is the raw material for the knowledge revolution of the Information Age. Without complete and reliable information, much of the benefit of information technology cannot be realized. Data warehousing and relational databases, geographic information and visualization systems, and extraordinary technological developments help us better understand our world and behavior of chaotic and complex systems that otherwise defy comprehensive human understanding. In such a technological environment, information is the fuel of our future. The benefits of the Information Age can only be realized if we have the raw materials on which it's essential systems depend: complete and accurate information used within the reasonable expectations of privacy.

As we have learned from such experiences as Y2K and various oil and gas disruptions, our technology systems are complexly inter-related. Technologies even depend on each other as we depend on them. Changes in one part of them tend to send cascading effects that carry the echo of that change throughout out systems. We continue to be surprised by this at our peril.

We also know that our government and the consumer economy is very info-dependent. 60% of our economy is consumer spending and marketing drives this. Our market economy itself depends on basic information equity and access or markets are not efficient. Government oversight and efficiency depends on enterprise wide data systems that cut across the traditional stovepipes of government agencies. The flow of information has become as vital as the flow of energy to our world. Neither the benefits of this information flow nor the costs of its restriction are fully apparent or even known, making necessary a deliberative approach to policymaking and some watchful waiting prior to action advisable.

HOW DO WE BALANCE PRIVACY AND ACCESS IN MAKING PUBLIC RECORDS POLICY IN THE ERA OF ELECTRONIC GOVERNMENT?

The following principles are a suggested starting place. The full text can be found in the attachment *The Public Record: Information Privacy and Access, A New Framework for Finding the Balance* by Cate and Varn.

1. Policymakers Should Identify and Evaluate Conflicting Interests

Decisions regarding privacy and access inevitably affect and are affected by other important interests. These interests are often socially valuable and deeply held. It is therefore essential that any policymaking process identify and examine those interests carefully to determine how they are implicated by a proposed law or regulation and to what extent they can and should be accommodated. In addition to the broad concepts of "privacy" and "access," those interests often include, but are not limited to, concerns about:

Equality: Equal and open access to public records helps level the playing field in such endeavors as issue advocacy, lobbying, and elections. It also gives small and start-up businesses access to some of the same databases as large and established players.

Freedom: Public records about the functioning of government, private individuals, and companies can be used to keep them in check so they do not impinge on the rights of others.

Participation: The more people know about their world and about government in particular, the greater the likelihood that they will increase the quantity and quality of their contributions to participatory and representative democracy.

Security: Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both privacy and access, cause explosive public reactions, and create governmental liability.

Economic Opportunity: A substantial portion of the current economy is in part dependent on the free flow of public records and limiting their use or availability will have economic consequences. Moreover, public and private records are the raw materials for the emerging economy and for the knowledge revolution of the Information Age.

Quality of Life: The use of information systems can free people from rote tasks and greatly speed transactions. Getting the amount of privacy one needs, however, also may affect quality of life.

Intangible Values and Uncertain Fears: A catchall value for things people like and dislike. Often we dress up our likes and dislikes in more eloquent terms, but often decisions and opinions are really based on this simple amalgamation of our feelings.

Efficiency: Efficient access to public records saves time, resources, and money. Without complete and reliable information, much of the benefit of information technology cannot be realized. However, we can also be so efficient as to impinge on individual freedoms.

Fairness: Is the process by which a law or rule is enacted, or by which a decision is reached, fair, and is the outcome fair to all of the parties involved?

2. Privacy solutions must respond reasonably to defined problems

Those privacy problems or harms used to justify restricting access to public records should be stated explicitly and should reflect reasonable expectations of privacy. The Supreme Court has long asked in the context of various constitutional issues, such as Fourth Amendment challenges to government searches and/or seizures: What expectation of privacy is implicated by access and how reasonable is that expectation? When evaluating wiretaps and other seizures of private information, the Court has inquired into whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.14 The inquiry regarding the reasonableness of the privacy concern should take into account three specific issues: (1) the sensitivity of the information disclosed; (2) the use to which the information is to be put; and (3) privacy protection afforded similar information in the past. These inquiries help prospectively arrive at a common-sense value on the privacy side of the access-privacy balance. Furthermore, the solution should go no further than is necessary to solve the problem: Access should be limited no longer and to no more data than necessary to protect privacy. Laws that purport to stop a harm to privacy but are ineffective harm both privacy and access. Such laws at once constitute an empty promise and a restraint on openness and freedom of information.

3. Limits on access to protect privacy should be effective and no more restrictive than necessary

The accommodation between access and privacy needs to be carefully crafted, so that we continue to permit as much access as possible without unnecessarily invading privacy. For example, both access and privacy interests might be served by delaying access to certain law enforcement records until a pending investigation is completed. In other cases, removing (known as "redacting") particularly sensitive information from documents otherwise made public might protect the individual's privacy interests and be preferable to denying access altogether. In no event should limits be imposed on access to, or use of, public record information to protect privacy if those limits will not in fact be effective in solving identified problems. Government should not impose broad limits on access to protect information privacy where effective, extra-legal mechanisms exist that permit a more sensitive and individualized balancing of access and privacy interests. The development of privacy seals and certification programs, anonymizing software, user-determined browser privacy settings, prominent privacy policies, industry codes of conduct, and technologies that allow persons to opt out of specified uses of some types of government records are examples of market responses to privacy concerns generally that diminish the need for government action by allowing individuals to protect effectively the privacy of data about them. Clearly, these and similar developments will not eliminate the need for government attention to information privacy, but the number and variety of these initiatives, and the speed with which they are emerging, suggest that they may supplant the need for at least some government actions to protect information privacy.

4. Privacy interests are limited to personally identifiable records

Access to government records that do not identify individuals should not be restricted on the basis of protecting privacy. Anonymous and pseudonymous records pose no meaningful privacy threat. Aggregate data can be used in ways offensive to the privacy concerns of some, but by far these concerns have been best addressed by market-based solutions and private sector codes of conduct. If government action is considered, it should be aimed at the behavior of the offenders and not the records themselves.

5. Enhancing state revenue is not a privacy problem

The government should not use privacy claims as a pretense for raising revenue or enhancing the competitive position of state-published information products. This principle does not suggest that the government cannot seek to recoup the marginal or even the operational cost of providing records. But levying excessive charges on

citizens to use a public infrastructure that is already paid for with tax dollars is wrong. Moreover, the government should not use claims of protecting privacy as a justification for restricting access to information for other purposes. This principle would seem to many so obvious as to not warrant stating, but many calls for privacy protection today are in fact seeking protection from other harms or are unrelated schemes for generating revenue.

6. Public information policy should promote robust access

Information policy should facilitate as much access as possible without harming privacy interests. The more robust the flow of data, the more robust the information infrastructure that supports both democratic processes as well as growth of our economy. This reflects the constitutional importance of open public records and the law in most U.S. jurisdictions today: access is presumed unless a specific privacy exemption applies. It also reflects the importance of the public record infrastructure to our polity and our economy. As noted above, it is often possible to target specific privacy harms and leave the public record infrastructure largely intact.

7. There should be no secret public records

An informed citizenry is essential to all checks and balances systems and that includes public record systems. The public should be able to easily discover the existence and the nature of public records and the existence to which data are accessible to persons outside of the government. In many cases, it may be desirable and appropriate for the government to inform citizens about who is using their public records and for what purposes. Obviously, access to records is not appropriate in all cases (one notable exception in many jurisdictions is investigative files before a criminal case is brought), nor will it always be feasible or advisable to provide information to citizens about the uses made of their records. But this principle recognizes that access not only serves broad social purposes, but also helps build citizen confidence in the public record system, improve the accuracy of public records, helps sharpen citizen understanding of privacy and access implications of the uses of their records so that they may respond appropriately, and contributes to educating all of us about the actual costs and benefits of public record access.

8. Not every privacy/access issue can be balanced

Despite the importance of balancing, it is not appropriate in every case. The courts have established that there are some instances where the societal interest in access is so great that it trumps all privacy concerns. For example, Congress recognized the overriding importance of access, irrespective of the significant privacy interests at stake, when it passed Megan's Law, requiring states to make publicly available the records of convicted child sex offenders for at least ten years after their release from prison. Congress believed that the societal interest in access to the record overwhelmingly outweighed the privacy interests, however great, of the convicted sex offenders. In other cases, information must be public to effectuate the public policy reasons for collecting it in the first place. One example of such a record is bankruptcy filings so that creditors have the opportunity to protect their interests and future creditors can accurately assess risk. Similarly, the privacy of some types of records is of such importance to our society that it outweighs access interests. Use of certain types of records, such as medical or individual tax records, causes such significant demonstrable harms that our society rejects that use even when there is a substantial desirable benefit. Productive use of other types of records causes such a visceral reaction that we restrict that use, as demonstrated by the recent outcry over digital driver's license photos. However, one must exercise caution in the application of this principle, as there are many false positives of this kind of reaction caused by sensationalistic journalism and unscientific or biased polling. It is also true that in most cases where a visceral reaction, rather than evidence of specific harms, prompts legislative action, that reaction precedes any understanding of the benefit of the use of the record so no true balancing process was used. Ultimately, policymakers must decide whether the harms are sufficiently clear and severe or the reaction sufficiently genuine and widespread to conclude that it is in the best interests of state or nation to close access to the public record.

9. Systems for accessing public records and, where appropriate, controlling their use should not be burdensome

The mechanisms for accessing the public records and for allowing individuals to protect the privacy of records concerning them should be easily accessible and no more burdensome than necessary. Information technology systems are emerging that may allow persons to opt out of specified uses of some of their government records. These important systems should not be exempt from the process of balancing the range of interests in the record against the privacy interests of the indi-

vidual. Moreover, these systems can be costly to run and government must account for this as a spending priority and a societal concern. It must balance the cost of such privacy and who benefits against the other priorities of the government, the public, and of those parties directly affected by the loss of access. In using this test it is rarely, if ever, feasible or justifiable to require a person to affirmatively determine the uses of their non-confidential records (known as opting in). This would involve permissions from each of person in the 100 million households in America for each record and/or for each use. The process of responding to countless requests for permission would make the solution worse than the problem.

10. Information policy must ensure the security of the public record infrastructure

The government must ensure that public records are protected from unauthorized access, corruption, and destruction. Public record security and integrity systems must be adequate to the task or their failure will defeat the goals of both information privacy and access.

11. Education is key

An informed citizenry is essential to the balancing process for both the individual choices they may make and in understanding the costs, risks, and benefits of privacy and access solutions. Government—assisted by industry, not-for-profit organizations, and the academic community—has a duty to educate the public about privacy and access issues. The more policymakers and the citizenry know about this issue, the more accurate and satisfying the balancing process will become.

12. The process for balancing access and information privacy should be sound

Government should have a process for balancing access and information privacy issues that is informed, consistent, and trusted by all parties. This process should be in place before one evaluates any new access or privacy issues.

WHAT ARE THE INFORMATION POLICY OPTIONS AND HOW CAN WE CATEGORIZE THE CHOICES?

First, there are four distinct issues that are often discussed as one and confusion is the result. Keeping the following separated will aid policymaking. The four different issues are:

- Privacy—the who, what, when, where, why, and how policies on data and records where our values are expressed and codified
- Security—the enforcement of privacy policies
- Integrity—maintenance and protection of records from accidental or purposeful alteration or loss
- Accuracy—quality assurance and a customer-friendly process to detect and correct errors

Of these four, security is the ripest for action. Government and private entities are beefing up security and hiring chief security officers, but our investments are lagging behind what a good risk/benefit analysis calls for. Better security programs, awareness, training, staffing, research, and so on are easy win-win areas for Congress and state and local government.The following are categories of other possible responses to any perceived gaps in our privacy or access policies.

Proactive Measures To Get Ahead Of Or More Directly React To The Problems

For example we could be investing more in law enforcement teams to directly combat identity theft and go after the bad actors instead focusing on restricting the information flows. Another area ripe for action is to fix our broken identity system by improving the birth, marriage, and death certificate issuance system and better coordinating them with our social security number issuance, driver's license, passport, and voter registration systems. The reason identity theft is rampant and many privacy problems occur is because we rely on an antiquated system of identity. A paper birth certificate, a social security number, your mother's maiden name, your city of birth, your name, and an address are the crumbling pillars of identity. All of these are easily stolen or forged and it is unlikely this genie will ever be put back in the bottle. These components of identity come from a time when people worked with and did business with their friends and neighbors, often on a handshake or a bare signature. There was no need to be able to prove you were whom you said: these people *knew you.* Today, we do business we people will never see or know. Many states, including mine, are moving forward with such systems as Public Key Infrastructure and digital signatures with optional biometrics to prove and repudiate identity. Iowa is also just beginning a project to strengthen our identity system to give our citizens greater security and more choices to prove and protect their identity. Congress should do the same. While this is not politically easy, we have

made such moves successfully in the recent past. Remember when driver's licenses did not have photos? Our citizens often renewed early to get the new photo licenses to make it easier to cash or write checks. We are ready for the next steps.

Organizational Infrastructure

There should be information policymaking entities in all three branches of government. These could be the CIO or another entity. The structures need to include both privacy advocacy and access advocacy in their makeup to provide a balanced approach. Privacy and policy enforcement entities are needed as well. Care needs to be given to creating policies that offer a hollow promise of protection because no effective enforcement policy, mechanism, and/or entity are created with the policy. Consideration must be given to likelihood of enforcement success and its cost to see if the information policy is cost effective or enforceable at all. A good question is: how far are you willing to go to detect violations? Will we use citizen trackers to help detect violations? Will we salt lists? Will we use stings, surveillance, and even undercover agents to detect violations? The allusion to the drug war is purposeful here as information is even more difficult to control. Be prepared for the cost of investment in money and in its invasiveness when you adopt information policy.

Services and Support

Government could go a long way to solving some of these problems with some public services. An example would be an identity theft advocate for the victims of this crime. This advocate would help the victim restore their good name and credit and could determine the authenticity of the victims claims and place a stamp of authority on their requests for record corrections to speed that process. They can also act as guide to help use existing law to repair the damage. Another service is that of gatekeeper to shield those for whom ordinary open records laws pose a special threat. Keeping one's name and address secret cannot be the pillar of security on which build a safety system for most people in a democratic society with a market economy. However, some people need special protection such as a battered spouse and a service that mediates contact with them to facilitate the normal business of living in our society would help address that problem directly. A final service would be to support P3P and other software-based solutions to make privacy choices practical and not unduly burdensome for transacting business with government.

Law and Policy

When considering any law or policy, it is helpful to consider each step in the public records process and narrowly tailor your solution to that step or steps that best effectuates your policy. The key steps are as follows:

- **Collect**—Weigh the burdens and benefits of collecting, using, managing, protecting, disseminating or keeping secret, storing, archiving, and preserving or purging the information. If you do not want the information in the public record, do not collect it in the first place.
- **Use**—What use will be made of the information, keeping in mind that not all uses nor their value can be judged in advance, and what is the value of that use.
- **Notice**—What kind of notice should be required to properly inform the customer. Consider more multimedia notices using , for example, distance learning tools instead of just print notices.
- **Choice**—If a choice is possible and if one is offered, how should it be exercised? Keep in mind that the transactional costs of opting in or out can be high and that for many government records (bankruptcy filings for example), opting is not an option.
- **Knowledge and Education**—Can you help people make more knowledgeable choices? North Carolina build such education into their K-12 curriculum.
- **Access**—To whom will access be granted and for what purposes?
- **Secondary use**—Many government programs such as the enforcement of child support orders require the secondary use of government records to work. For example, tax refunds and in some states, professional licenses are withheld for delinquency. Some unauthorized information reuse by government is inevitable. Still, consider whether government or others will be allowed such use.
- **Downstream use**—Most public records not restricted any more than any free speech is in our society. Consider both the value of this and the cost before restricting such use and how it would be enforced.
- **Dispose**—You can deal with sensitive information such as credit card numbers by making it a transactions collection only and not keeping it after that step. Like the credit card number, get rid of information that government does not need to do business or administer the laws.

- **Redact**—Eliminate sensitive information from records instead of restricting the entire record. This often solves the privacy problem and preserves the benefits of robust access and openness.
- **Expunge**—This tool has been used in the criminal history area for both adults and juveniles. Consider whether other records should be handled in the same way.
- **Store**—This is both a decision and a security issue: should you store it, for how long, and how will it be protected?
- **Archive**—Finally, our archival policies should be considered in light of both the interest of preserving history and in protecting privacy. The change from paper to electronics may lead one to make different archival decicions.
- **Market Solutions**—Consider whether government action is necessary or whether the market has or can develop a solution. Companies will react when their customers react and looking for market failures may be a more productive use of precious policymaking efforts. Remember also that good customer service often requires use personal information and many people want that kind of service. Those of us who grew up in small towns expect our merchants to know their customer and what we need. Technology makes that possible in mass markets and it is very popular. Those who do not want to be treated this way usually have an alternative if the company is smart. If they are not, there is a burgeoning privacy industry that can help you stay anonymous and even broker you personal information for your gain.
- **Rights**—A final tool is all of the existing and newly created statutory and constitutional rights. Consider whether people can protect their own rights with civil suits and whether it would be better to let the courts sort out some of the hard questions case by case and later codify case law as we have in many other areas.

DRIVER'S LICENSE PROTECTION, VOTER REGISTRATION, LOCAL RECORDS, IDENTITY AND STATE AND LOCAL ACTIONS ON PRIVACY

Finally, I have been asked to address some of the federal and state laws that relate to privacy. First, the DPPA has been implemented by the states as mandated. However, it is questionable whether the benefits were worth the cost. We must consider one of the main premises of the law and the impetus for its consideration: that a person's address can and should be a secret to ensure ones safety. As already noted, protecting one bit of commonly available information is not a good foundation for personal security for most persons. If you rely on such remedies alone you will not achieve the desired result and you will have cut off valuable uses of the information. DPPA has been educational for the citizens, but it is questionable whether informed choices are being made on the opt-in provisions. Furthermore, given the exceptions in the law and the commonness of some of the "protected" data, it is also questionable whether citizen expectations of privacy are realistic or accurate.

Second, voter registration systems are being studied and updated nationwide. The Motor Voter provision has encouraged more citizens to register, but antiquated data systems have hindered the smooth or accurate addition of these voters in many states. Investment in the basic infrastructure of democracy continues to be a crying need, but the window of opportunity to act may be partially closed with the financial troubles many states are currently experiencing. Whether excuse or honest attention to other priorities (such as HIPAA compliance), voter registration modernization may slip through the cracks. Federal investment in matching grants would be a wise choice.

As far as voter registration systems and privacy is concerned, consider that voter registration privacy may be an oxymoron. Without robust open access, our democracy does not work. Without adequate identity controls, it cannot be trusted. If the addresses of your constituents are secret, how can you serve them, persuade them, or reach them?

Third, local records are bedrock of government's information infrastructure. The basic building blocks of our data are made and kept there. Yet, the level of investment in these systems, their security, and their modernization is extremely varied. Much is made of countering threats to our national infrastructures but little attention is paid this vital link in our government system and our economy. Those local governments who are not keeping up are a drag on privacy, security, access, and e-government. Consider ways to encourage them, help them, and establish basic voluntary minimum requirements to give local records advocates and administrators a spur to action.

Fourth, to reinforce the importance of non-federal records, it should be noted that the very fact of civic and economic citizenship for most Americans is established and

extinguished by the birth, marriage, and death records created by state and local government. These foundational elements of our society are badly in need of modernization, coordination, and sound policy making around their creation and use.

Finally, most states are now fully engaged in privacy, security, access, and e-government efforts. Substantial work remains, but much is being accomplished. Federal pre-emption while attractive for reasons of uniformity would cut Congress off from these laboratories of democracy in a case where they are needed most. Let them work. Offer financial encouragement and assist them to share best practices. Let them achieve and make mistakes and learn from both. The issue of information integrity (which includes disaster recovery and business continuity) constantly suffers from a classic risk management dilemma: how much do you spend to avoid a catastrophe and how do you convince people to spend the money today when there are so many pressing needs. We all worry about our other infrastructure—sewers, water, highways, and buildings—a lot more than we worry about our information infrastructure. We need to continue to grow our investment and partnerships in this area. Finally, a federal-state-local-private-sector partnership is warranted in the area of accuracy. We do not have as many good models nor are the investments being made in either quality assurance or systems for finding and fixing inaccurate information held in public and private records.

Mr. STEARNS. Thank the gentleman.

Mr. Torres, you are recognized for 5 minutes.

STATEMENT OF FRANK TORRES

Mr. TORRES. Mr. Chairman, Congressman Towns, Congressman Shimkus, on behalf of Consumers Union, thank you for this opportunity to speak with you about privacy today. I'm going to try to put a little different perspective on it, looking at it from a consumer's perspective.

The state of privacy in America today is not very good. Every day, consumers are forced to give up their privacy to get products and services. Often consumers don't even know the information about them is being collected and even if they did, they couldn't do anything to stop it. Soon, as we found out, your TV will now be watching, your cell phone will give others your location, your computer software may even turn on you, sending out data about you and your family to the world. Web bugs and cookies are already the norm. The filters used by parents and schools have turned out to be data collection devices. Kids on their home computers and students in their classrooms aren't even safe from prying eyes.

Industry was unable to keep its promise to self-regulate when it came to kids, so Congress passed COPPA. Now we find that some websites don't like the law and are ignoring it. The Annenberg School at the University of Pennsylvania came out with a very compelling study showing that people simply aren't complying with the law. To us, there's a problem in the marketplace when Congress can't even protect America's kids from these prying eyes in the classroom and at home. Simply put, the marketplace will not provide adequate privacy protection for America's consumers. So if consumers want privacy, Congress must act. But for the most part, it really hasn't.

We've talked a lot today, there's been a lot of discussion about a comprehensive approach to privacy and something came out time and time again. And as the gentleman from AT&T pointed out, their philosophy is let consumers choose. Well, that would be a foundation for a comprehensive privacy law. Let consumers choose. Notice isn't enough. As Richard Smith testified, the notice that you got on the TiVo didn't fully explain what they did.

Consent shouldn't be looked at as a restriction, rather it would help foster competition. If a company is so confident in its products then why not convince the consumer to allow it to have access to the consumer's information to collect it to provide even better products and services?

Unfortunately, there are no laws today protecting privacy online. There are no laws that begin to contemplate emerging technologies like spyware. Gramm-Leach-Bliley is weak and full of loopholes and the medical privacy protections that should have been put in place by now have now been put on hold after industry resistance.

Now thanks to happenstance, and perhaps we need some more Supreme Court nominations to come before Congress to get better privacy protections. Consumer cable and video viewing habits are now better protected than sensitive medical and financial records, but the laws protecting what we watch are subject to attack.

We've been told by industry that there are savings to be had by all this flow of data and that goes into the cost benefit analysis that I want to address briefly because what's happening in reality for consumers doesn't kind of match what we're being told.

We're being told information flow will allow for targeted marketing. Well, just because it's targeted doesn't mean that it's not still junk mail for the consumer and again, it's not that a consumer couldn't agree to accept this, to agree to have their information being used for targeted marketing, but why not ask for the consumer's consent first?

The Washington Post reports today that more and more of our Nation's children are being targeted with credit card solicitations. They're trying to hook our kids early on credit. Is this the benefit of information sharing? Is this what Gramm-Leach-Bliley was all about? Is this what targeted marketing is all about? This is the benefit that they're targeting our kids with credit card offers?

We are told that data is also needed to determine risk and yet Freddie Mac and Fannie Mae and industry sources themselves estimate that up to 50 percent of consumers in the higher price subprime market could actually qualify for less expensive products. What good is information sharing doing those consumers?

Companies say information is needed to avoid identity theft, if there's nothing today preventing companies from using the vast amounts of information that they already have to deter fraud. Instead, information seems to be given to just about anyone who calls up, including a dishwasher who is impersonating private investigators or whatever he was doing and therefore getting credit extended to him in the names of Oprah Winfrey, Warren Buffet. Tiger Woods recently had his identity stolen. I would have loved to have been a fly on the wall listening to somebody call up saying I'm Tiger Woods, please send me a credit card with no checks being done and the credit card being sent.

In some cases, a simple phone call could have prevented this identity theft. Instead, the victims are now spending years trying to clear their good names. If companies can't use the information that they already have, how is increasing their ability to collect more information going to help stop this problem?

Companies also say information will help lower prices for consumers, but we're not seeing this. Banks are constantly raising fees. They're partnering with PayDay and predatory lenders to offer, in fact, higher cost products. When banks find out that you're late on your electric bill or your gas bill, they can actually jack up your interest rate on your credit card, even though you've made all your credit payments on time. This isn't a good use of this information flow.

In conclusion, let me say that we believe Congress needs to take a comprehensive look at privacy legislation. Otherwise, it's an information grabbing free-for-all, with little benefit to consumers. So in the end, consumers are waiting to see what Congress is doing and we appreciate these series of hearings. We're also wondering what the new Administration will do to protect our privacy.

A new survey by the Pew Foundation finds that the majority of Americans, 70 percent of on-line users want Congress to pass on-line privacy laws. Consumers Union hopes that Congress will act and the President will keep his word when he said that he believes in strong privacy protections and the need to put consumers in control of their information.

Thank you, Mr. Chairman. I'd be happy to answer any questions.

[The prepared statement of Frank Torres follows:]

PREPARED STATEMENT OF FRANK TORRES, LEGISLATIVE COUNSEL, CONSUMERS UNION

Consumers Union [1] appreciates the opportunity to testify before the Subcommittee on Commerce, Trade, and Consumer Protection. This hearing on An Examination of Existing Federal Statutes Addressing Information Privacy provides a needed forum to discuss the lack of meaningful privacy protections for American consumers.

The first part of this testimony discusses privacy in general. The second part goes into greater detail on specific issues: online privacy, children and student privacy, subscriber privacy, financial privacy, and medical privacy.

THE STATE OF PRIVACY

Consumers are fed up with aggressive intrusions on their private lives. Often a consumer is forced to provide personal information to obtain products or services. Many times information that has been provided for one purpose is then used for another reason, unbeknownst to the consumer. Financial institutions, Internet companies, and marketers have been caught crossing the line.

Some members of Congress are not only shining spotlight on privacy, but also working to ensure that consumers are told about how and why personal information is collected and used, provided access to that data, and given a choice in the matter. But real protections have been slow in coming.

Instead, the right to be left alone appears to have been trumped by the pressure exerted by businesses to protect and expand their ability to gather personally identifiable information from consumers. No part of life is left untouched by data collection activities. Financial and medical records, what you buy, where you shop, your genetic code, are all exposed in a privacy free-for all. Complete strangers can, for a price, have access to your most intimate secrets.

This means that consumers have lost control over the ability to being left alone. Often, consumers have no choice in whether or not information is collected and no

[1] Consumers Union is a nonprofit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education and counsel about goods, services, health, and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union's income is solely derived from the sale of *Consumer Reports,* its other publications and from noncommercial contributions, grants and fees. In addition to reports on Consumers Union's own product testing, *Consumer Reports* with approximately 4.5 million paid circulation, regularly, carries articles on health, product safety, marketplace economics and legislative, judicial and regulatory actions which affect consumer welfare. Consumers Union's publications carry no advertising and receive no commercial support.

choice in how it is used. Today, any information provided by a consumer for one reason, such as getting a loan at a bank, can be used for any other purposes with virtually no restrictions.

Do consumers care? You bet they do. According to a Forrester Research survey of online users, 67 percent said they were "extremely" or "very" concerned about releasing personal information over the Internet. It is estimated that those fears may have resulted in as much as $2.8 billion in lost sales for Internet retailers in 1999. The lack of privacy is costing business. AARP found that 93% of those surveyed believe that any personal information provided during a financial transaction should remain the property of the consumer and that the information should not be shared with other businesses without the permission of the consumer.

Last year, a Business Week/Harris poll shows that 92% of Internet users are uncomfortable about Web sites sharing personal information. 57% favor the government passing laws on how personal information is collected and used. And many people are uncomfortable with the creation of profiles. 82% said they were not comfortable with linking their identity with personal information like income, credit data, and medical information.

The ability to collect, share and use data in all sorts of ways boggles the mind. Consumers, in many cases, aren't even aware that data is being collected, much less how profiles about them are created. The information collection overload is particularly troublesome when it becomes the basis for decisions made about an individual—like how much a product or service will cost.

What protections do consumers have today? Not many. For all the talk about giving their customers what they think they want, the marketplace is not willing to give their customers what they really want—privacy. Privacy laws are either nonexistent or are so riddled with loopholes that in most cases consumers will not have to be told that their sensitive information is being shared, or be given the ability to stop the sharing of their information.

Privacy invasion isn't only happening online. Cross industry mergers and consolidations have given financial institutions unprecedented access to consumers' personal data. Technology has made it possible and profitable to mine that data. No law prevents financial institutions from using data to choose between desirable borrowers and less profitable consumers the institutions may want to avoid. Special software helps guide sales staff through scripted pitches that draw on a customer's profile to persuade the account holder to buy extra, and in some cases junk products

The much ballyhooed privacy provision of the Gramm Leach Bliley Act does not protect consumers' privacy. And because the underlying bill is bad, the implementation of regulations provides little hope for consumers seeking to keep their personal information private. While states were given the ability to enact stronger protections, those efforts have met fierce resistance by the financial services industry.

Consumers across the country are receiving privacy notices from their financial institutions. These notices were required under GLB. Consumers should respond by opting out of the use of information to send a message that they care about their privacy. Unfortunately these opt outs, in reality, will do little or nothing to prevent the sharing of your information with others.

We need stronger laws to put power and choice in the hands of consumers regarding the collection and use of their personal information.

Some web-based businesses already seem to be willing to move beyond the privacy wasteland where GLB left consumers. There no longer appears to be a question, for some, of whether consumers should get notice, access, and control over their information. The challenge is how to effectively put these principles into practice.

What about privacy policies? Won't those do the trick? Privacy policies are not a substitute for privacy protections, especially when some companies don't even follow what is in their policies. Just because a company has a privacy policy does not mean that they follow Fair Information Practices. And consumers are skeptical about self-regulation. Only 15% of those surveyed in the Business Week poll supported letting groups develop voluntary privacy standards. Nor has industry shown the will power to adopt adequate self-regulatory programs.

Some tout the use of technology to allow consumers to choose their preferences—even "opting-in" using a privacy thermometer. Will the technology allow a consumer to shut-out all intrusions? Unfortunately, the usefulness of technology often depends on knowledge of the user. Technology may be of some use, but may prove lacking where it unfairly pushes the burden on the often-unsuspecting consumer. If you are not in the know, you will likely lose your privacy because you won't know how to keep it private. And if the preferences can be circumvented, then the usefulness of a technological solution without baseline protections will be completely lost.

Where is all this going? The marketplace is changing daily. The Wall Street Journal reports that Time Warner has the names, addresses and information on the reading and listening habits of 65 million households. USA Today says Time Warner has access to information about its 13 million cable subscribers and from its other businesses, like Time and People magazine. With so much information, how will the competitiveness of the marketplace be impacted by this merger? Will companies who seek to operate under a higher privacy standard be at a competitive disadvantage and unable to compete against a larger entity that is able to make unrestricted use of the personal information it obtains? Is this the future? Now imagine a Time Warner/AOL/Bank of X.

Will consumers benefit from all this data sharing? Financial institutions promised that in exchange for a virtually unfettered ability to collect and share consumers' personal information, that consumers would get better quality products and services and lower prices. This is why, they claimed, consumers shouldn't have strong privacy protections like the ability to stop the sharing of their information among affiliates, or access to that information to make sure its accurate. Let's look at reality.

Bank fees for many consumers continue to rise. Information about financial health may actually be used to the consumer's determent if it is perceived that the consumer will not be as profitable as other customers. Both Freddie Mac and Fannie Mae say between 30 and 50% of consumers who get subprime loans, actually qualify for more conventional products, despite all the information that is available to lenders today. Credit card issuers continue to issue credit cards to imposters, thus perpetuating identity theft, even when it seems like a simple verification of the victim's last known address should be a warning. Instead of offering affordable loans, banks are partnering with payday lenders. And when do some lenders choose not to share information? When sharing that information will benefit the consumer—like good credit histories that would likely mean less costly loans.

Chase Manhattan Bank, one of the largest financial institutions in the United States, settled charges brought by the New York attorney general for sharing sensitive financial information with out-side marketers in violation of its own privacy policy. In Minnesota, U.S. Bancorp ended its sales of information about its customers' checking and credit card information to outside marketing firms. Both of these were of questionable benefit for the bank's customers. Other institutions sold data to felons or got caught charging consumers for products that were never ordered.

Maybe the right approach is to let institutions that want a consumer's information to be put in a position to convince that consumer that some benefit will be derived from a willingness to give that information up to the institution. Such an approach may increase trust in financial institutions and let consumers have control and choice over their own personal information. The same technology that enables vast amounts of data to be collected can be used to give consumers access to that data. It is a simple thing to tell consumers what is collected and how it is used.

Sound and comprehensive privacy laws will help increase consumer trust and confidence in the marketplace and also serve to level the playing field. These laws do not have to ban the collection and use of personal data, merely give the consumer control over their own information.

SPECIFIC PRIVACY ISSUES

The Lack of Online Privacy

A May 2000 *Consumer Reports* survey of web sites, *Consumer Reports Privacy Special Report, Big Browser is Watching You,* shows that consumers' privacy is not being protected online. The report also shows that privacy notices at several popular sites are inadequate and vague. This data, as do other recent web surveys, shows the state of consumer privacy online continues to be dismal. Not much has changed since that survey was first done.

Consumers Union has urged Congress and the regulators to reverse their prior reliance on industry self-regulation and recommend that legislation is both appropriate and necessary to protect the privacy of on-line consumers.

The *Consumer Reports* survey evaluated the placement of tracking devices at 28 sites. The privacy policies at six heavily trafficked commercial web sites were also examined.

Among the findings of the report:

- Even the activities of the most casual Internet users are carefully monitored by advertisers—often without the users knowledge or consent. Marketers are able to amass personal data about what you buy, what you read, what ails you and what you are worth.

- Most web site visitors may be unaware that the simple act of viewing a site's home page can trigger the placement of a cookie by an ad network with whom they never consented to have a relationship.
- Trying to block cookies resulted in some sites generating as many as 28 attempts to implant a cookie before displaying the home page of the site.
- There are troubling shortcomings in the privacy policies of popular sites: inadequate notice, vague disclosures, and unproven "seals of approval."

It is apparent that self-regulation has done little to protect privacy. Companies continue to pursue ever more invasive collections of personal information. And there is no legal safeguards that limit what data collectors can gather. Inadequate notice of privacy policies that may or may not address fundamental Fair Information Practices leave consumers vulnerable and ill-equipped to make informed choices. Lack of strong privacy laws has resulted in continued intrusions into consumer privacy, little accountability, and no assurance that other firms will not engage in similar practices in the future.

Because of the failure of the industry to police itself, Consumers Union supported the Federal Trade Commission recommendations to Congress that legislation is needed to protect the privacy of consumers on the Internet. Strong protections now will not only curb privacy intrusions, but also have the benefit of increasing consumer confidence when choosing to go online.

Protecting Children

Consumers Union recognizes the benefits of the World Wide Web, especially in opening doors to the world through access to a variety of sites containing a lifetime of information. But it is also a medium where children can be placed at risk, especially when asked to provide personal information about themselves, their family and friends. With the ever expanding and increasing use of the World Wide Web, by both adults and children, it was appropriate and timely that Congress passed the Children's Online Privacy Protection Act of 1998 (COPPA), specifically placing the control of information collected from and about children with parents.

COPPA said that online protection for kids must:

- Not exploit kids' inexperience and vulnerability. Attempts to do research or glean personal information shouldn't be disguised as entertainment, and prices shouldn't be used to induce kids to provide personal information.
- Be widely available and easily implemented, even by adults who aren't computer literate.
- Provide a foolproof way to communicate directly with parents, rather than rely on having kids get permission to visit a site.

As the Federal Trade Commission adopted rules to implement COPPA, Consumers Union made the following comments:

- Children must be protected against the online collection of personal information without a parent's prior informed and verifiable consent.
- Close potential loopholes in the proposed rule that could allow operators to circumvent the intent of COPPA.
- Ensure that parents receive a simple and comprehensive notice of policies, that information on the collection, use and dissemination of the information be complete and accurate, and that there be a means to verify parental consent in cases where a parent makes an informed choice.
- Ensure that information previously collected from children is given the same protection as future collected information.
- Exercise care in providing a safe harbor for self-regulatory efforts

Consumers Union fails to see any compelling commercial interest to allow a website to collect personal information about children without their parent's knowledge or consent. A commercial website, under the proposed regulations will, in fact, be able to collect and use such information. It simply has to inform the child's parents about what type of information will be collected, how it will be used, whether it will be shared, and then obtains the parent's consent. Congress was clear in it's intent when it passed COPPA—that the interests of children and not that of industry should be protected.

A recent study by the Annenberg Public Policy Center of the University of Pennsylvania found the most children's websites are not following the spirit of COPPA. Moreover, the study found that the privacy policies that exist on many sites are often very difficult to read and are missing key elements. While children's sites that collected personal information had a link from their home page to their privacy policy, many skirt COPPA by not prominently displaying those links.

Even more troubling was that the researchers found the policies too complex to understand. Many were determined to be either too short and vague or too long and

confusing to be read in a brief period of time. The researchers questioned whether companies expect or want parents to read their policies.

The lack of compliance with COPPA highlights the need for further Congressional action. If children are not safe when they go online despite the passage of COPPA, something more needs to be done. Failure to comply with COPPA should not be taken as sign that children using the Internet should not be protected. Rather, it shows that Congress should demand swift enforcement of the law, strengthen it's provisions, and send a strong message to industry groups who go after America's kids.

In addition to protecting children online, students in our classrooms should not be forced to submit to data collection of personal information by business interests so that those businesses can then turn around and use that data to target kids. Today, companies are being allowed easy access to America's children through our schools:

- A California company provides schools with free computers, software, and access to certain web sites. In exchange, the company monitors students' web browsing habits and sells the data to other companies.
- Children in a Massachusetts elementary school spent two days tasting cereal and answering an opinion poll to help the company sell to kids.
- Children in a New Jersey elementary school filled out a 27-page booklet called "My All About Me Journal" as part of a marketing survey for a cable television channel.

Schools should not usurp parent's authority when it comes to the privacy of children weighed against purely business interests. The taking of information for non-educational commercial purposes effects students outside the classroom, especially because no guarantees can be given about how the information collected may eventually be used and by what types of companies.

Protection of Subscriber Privacy

The privacy of personal information is a growing concern with the integration of various technologies. Consumers Union agrees with the Federal Communications Commission (FCC) that the privacy provisions of the Communications Act apply to cable operators and their affiliates.

The Communications Act provides that at the time a cable operator enters into an agreement to provide any cable service "or other service" to a subscriber, and annually thereafter, the cable operator shall inform the subscriber of, among other items, the nature of personally identifiable information the cable operator will be collecting, the nature of the use of the information, and the nature and purpose of any disclosures of that information.

The Communications Act also provides that a cable operator may not use the cable system to collect personally identifiable information. The cable operator cannot disclose personally identifiable information without the prior written or electronic consent of the subscriber. The statue defines "other service" to include any wire or radio communication service provided using any of the facilities of a cable operator that are used in the provision of cable service.

Financial Privacy Not Yet a Reality

The Gramm-Leach-Bliley Act (GLB) falls far short of providing meaningful privacy protections. Loopholes in the law and in this draft rule allow personal financial information to be shared among affiliated companies without the consumer's consent. In many instances, personal information can also be shared between financial institutions and unaffiliated third parties, including marketers, without the consumers consent. Other loopholes allow institutions to avoid having to disclose all of their information sharing practices to consumers. In addition, the GLB does not allow consumers to access to the information about them that an institution collects.

With the passage of the GLB, the financial marketplace is poised to undergo rapid and profound changes, including the consolidation of industries. One consequence is that personal financial information has become a marketable commodity, with banks, insurance companies and securities firms knowing, and having the capacity to know, more about an individual consumer than ever before. Not only is this information used to market products and services to consumers, it can be used to make decisions about the cost and availability of those products and services.

Consumers have reason to be concerned about how their private financial information is being collected, used, shared and sold. Under the GLB there are no limits on the ability of a financial institution to share information about consumers' transactions, including account balances, who they write checks to, where they use a credit card and what they purchase, within a financial conglomerate. Because of loopholes in GLB, in most cases sharing a consumer's sensitive information with a

third party is allowed too. All the exceptions created by GLB make it difficult to come up with a list of circumstances where personal financial information cannot be shared.

Here is why the GLB fails to provide privacy protections:

- **Limited notice provisions.** The notice provisions merely require that an institution provide consumers with the institution's privacy policy, which could simply say "We share your information with affiliates and third parties." Financial institutions would only have to provide *general* information about the type of information that is collected and with whom it is shared. A consumer would not have to be told how their information is being used. In some cases the proposed regulations do not require that an institution provide a consumer with any notice at all, such as when the information collected is used to service an account.
- **Opt-out to "nonaffiliated third parties" only.** GLB's limited third party opt-out does not apply at all to internal affiliate sharing—affiliates can still share and sell information. Consumers will have no ability to stop it.
- **Loopholes gut the already limited opt-out requirement by allowing information to be shared with "nonaffiliated third parties" under most circumstances.** Even if a consumer wants to opt-out, information may still be shared with third parties offering financial products on behalf of or endorsed by the institution or pursuant to a joint agreement between financial institutions. Thus, financial institutions can share customers' information without notice to the customer or permission from the customer.
- **No consumer access.** The law does not allow a consumer to have access to the information collected, or the ability to correct erroneous information.

Here is what consumers should have when it comes to privacy protections:

- **Notice:** Financial institutions should inform their customers in a clear and conspicuous manner when they plan to collect, use and/or disclose personally identifiable information, and customers should be told the intended recipient of the information and the purpose for which is will be used. Notice should be about the sharing of information with all entities, both internal and external, and for any reason, including the servicing of accounts.
- **Access:** A customer should have access to all personally identifiable information held by the financial institution to make sure it is accurate, and complete and customers should the ability to correct erroneous information. These rights should not only be limited to account information, but should extend to any dossiers, profiles or other compilations prepared for sale or sharing with third parties.
- **Consent:** A financial institution should receive prior affirmative consent of the customer before it uses and/or discloses that customer's information for any other purpose than for which it was originally given. No customer should be denied, or forced to pay a higher price for, any product or services by a financial institution for refusing to give consent to the disclosure of the customer's personal information except where necessary to determine eligibility for a specific financial product or service.

Consumers should have the right to be fully and meaningfully informed about an institution's practices. Consumers should be able to choose to say "no" to the sharing or use of their information for purposes other than for what the information was originally provided. Consumers should have access to the information collected about them and be given a reasonable opportunity to correct it if it is wrong. In addition to full notice, access, and control, a strong enforcement provision is needed to ensure that privacy protections are provided.

Medical Privacy

When Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) the Department of Health and Human Services (the "agency") was directed to develop and implement rules to protect the privacy of Americans' health information by February 2000. More than a year later regulations have not been implemented. The rule followed normal rulemaking procedures. All interested parties had ample opportunity to provide comment. In fact, the comment period was extended to provide additional time to submit views. The comments were given due consideration and a final rule was published. The agency has now used a procedural technicality to reopen the rule for additional comments.

The *Final Standards for the Privacy of Individually Identifiable Health Information,* 65 FR 82462 (December 28, 2000) is a significant step towards restoring the public trust and confidence in our nation's health care system. Critics of the rule are urging the agency to scrap the rule or otherwise delay its implementation. The agency is being urged to weaken it by taking away the rights of patients to consent to the sharing of their information, denying patients the right to access their own

records, creating larger loopholes in the rule, and allowing holders of medical information to share their patients' data with others without any responsibility or accountability. The rule should not be scrapped or delayed. If changes are made to the rule those changes should strengthen, not weaken, the medical privacy protections.

But nothing has changed since the rule was finalized that diminishes the need for strong medical privacy protections. Medical information continues to be used for inappropriate purposes. The rule itself highlights a number of cases where private medical information was released for profit and marketing purposes—completely unrelated to the treatment of those patients. A recent *USA Today* editorial further highlights the consequences of a failure to protect medical privacy—an employer firing an employee when they got the results of a genetic test; release of medical records to attack political opponents; and hackers getting access to health records from a major University medical center (*USA Today,* March 20, 2001).

Patients should not be put in the position of withholding information or even lying about their medical conditions to preserve their privacy. Those seeking medical treatment are most vulnerable and should be allowed to focus on their treatment or the treatment of their loved ones, rather than on trying to maintain their privacy. It is unfair that those citizens must be concerned that information about their medical condition could be provided to others who have no legitimate need to see that information.

The rule is simple.

- Patients are told in plain English how their medical information is used, kept and disclosed.
- Patients are allowed to see their medical records and get copies of those records if they want. Patients are also allowed to have inaccurate information corrected.
- Patients are allowed to consent to the disclosure of their health information in most circumstances, including non-medical or non-treatment related purposes. Companies should have to defend their reasons for wanting access to that data. If those companies are unable to convince patients to consent to the use of their information, they should not be able to circumvent the patient's choice.
- The rule limits the use of an individual's health information to health purposes only with few exceptions.
- The rule says that hospitals and other providers must adopt privacy procedures, train employees about those procedures, and provide a process if those procedures are violated.
- The rule holds the hospital and other health care providers accountable if patient health information is misused.
- The rule only requires that reasonable safeguards be used. Hospitals will not have to erect soundproof walls, as some critics have charged.
- The rule is flexible. People will still be allowed to pick up prescriptions for family members. If further clarification is needed, the rule allows the agency to simply issue guidance. Because the agency is allowed to act if needed, this issue and similar issues can be resolved without weakening or delaying the rule.
- The rule allows information sharing for treatment purposes. The quality of patient care will not suffer. In fact, by increasing trust between the doctor and patient, the rule will likely increase the quality of care.

Medical information in the context of financial services has also been considered. Last year, Congressman Leach, then chair of the House Banking and Financial Services Committee introduced the Medical Financial Records Privacy Protection Act that would have prevented financial institutions from sharing medical financial records without customer consent. Further, the bill would have prohibited financial institutions from using consumer's medical information in providing credit. The bill was voted out of the House Banking Committee but Congress failed to act on the bill prior to their adjournment.

The Leach Medical Financial Privacy Protection Act would have:

- Required financial institutions to obtain customer's affirmative consent before disclosing individually identifiable health information to an affiliate or non-affiliated third party.
- Prohibited a financial institution from obtaining or using individually identifiable health information in deciding whether to issue credit, unless the prospective borrower expressly consents.
- Provided consumers the right to inspect, copy, and correct individually identifiable health information that is under the control of a financial institution.

Mr. STEARNS. Thank you.

Mr. Zuck, your opening statement.

STATEMENT OF JONATHAN ZUCK

Mr. ZUCK. Mr. Chairman, members of the subcommittee, thank you very much for allowing me to be here. Since they're not here to defend themselves, I'd just like to go on record and say I love my TiVo. So if anybody wants to talk endlessly about the benefits of TiVo, I'm happy to do that.

I am currently the head of a high tech trade association that represents mostly small businesses, a voice that's often not heard and often a constituency that's most affected by compliance costs with regulation, etcetera because those same economies of scale, when applied to small businesses often put them out of business. My background is actually as a software developer though and I've built applications for Freddie Mac, American Express and in fact, the program that authorizes the majority of the checks written by the Federal Government is something of my creation. So I can affirm that privacy and data security is certainly not a new issue to the on-line world.

One of the things we learned in the software industry is that for everything we try to do there are goals, a process and an outcome associated with what we're trying to create. And one of the things that we learned is that sometimes when we slip up on the process, it creates a disparity between the goals and the outcome of the project at hand. One example of that was the Children's On-line Privacy Protection Act and that's what I've been asked to talk about here today.

Mr. Plesser talked a little bit about what some of the tenets of that act are, so what I want to do is just talk a little bit about what some of the unintended consequences were associated with the passage and then also the follow-on rulemaking associated with COPPA.

I'd like to refer to that Annenberg study that's actually come up a couple of times today that talks about noncompliance. If you look at it, there's actually some contradictory things. This notion that sites are not complying actually says that while 90 percent have privacy policies, but some of them are too short and vague, others are too long and complex. So what you have is a situation, a Catch-22 in which creating something which is clear is not enough information. Something which is not enough information is unclear. And so what we find is that in a regulatory environment, compliance alone is not actually going to get you to what you're trying to accomplish. You're not actually affording the protections that you were attempting to afford and instead, creating complexity because of people wanting to cover themselves down the road. So it's not necessarily a true protection to have compliance.

The other issue associated with COPPA has to do with the sort of exclusion of adult sites. It actually creates a bias against sites that were legitimately trying to create children's content and I don't envy your position as lawmakers in trying to balance different objectives, but one of the objectives at the outside is to increase consumer confidence in children's sites, etcetera and to protect children on-line. It's hardly a protection of children to push them toward lying about their age on an adult site, where it's actually easier for them to go on-line, easier to get an e-mail account than it is on a site that was actually set up specifically for children.

So these authentications that are required from parents present another interesting issue. You want to require to parents, authenticate that they're parents and that they're adults, etcetera, which requires sharing a lot of information that sites weren't otherwise ordinarily collecting. So in fact, it actually forces the collection of additional information in order to protect the privacy of people that were otherwise operating anonymously on-line.

The other issue that's important always to raise in the cost benefit analysis that you raised, Mr. Chairman, is some of the costs of compliance with COPPA. FreeZone estimated that their costs were ranging about $100,000 a year; Zeeks, something like $200,000 a year. And ZD News did an overview study and said that costs could range as high as half a million a year to comply with these regulations that were imposed by COPPA and the follow-on rulemaking. What that has done is actually led businesses to drop their practices or go out of business again, not necessarily furthering the goals of creating the law in the first place.

The other issue associated with process is that we saw an overboard definition of collection of information. The law specifies that before sites can collect and use information, they need to get parental consent, but when that was handed over to the FTC it actually turned into the monitoring of chat rooms and things and so sites that, in fact, were not collecting much less looking at information, are now required to have monitors in chat rooms and people on phones with respect to different sort of peripheral information that they weren't even trying to collect, which again creates costs that I don't think were intended by the original language of the law.

So finally, you have to talk about what are some of the things that are happening in the industry that can help to protect privacy and empower consumers. One thing is that there's technologies that are coming into being. You've heard a little bit about the platform for privacy preferences or P3P that's actually an industry-wide standard that allows a browser essentially to read the privacy policy of a website, so that if you've set preferences in a browser, the browser then identifies whether or not those preferences match up to the policy of the website so that you're not left reading through the legalese of a privacy policy. And there are also on-line wallets and on-line information brokers, things like Microsoft's Kids Passports. There's kids' credit cards, etcetera that facilitate the central use of information and then the choice about how that information is used by individual sites. And finally, something that we at the Association for Competitive Technology have always tried to promote is just plain old consumer education. The more that people know about the on-line world, the more they use the on-line world, the more consumer confidence rises. We have to ask ourselves whether consumer confidence is best increased through the empowerment and education of consumers or through regulation that might not, in fact, protect their interests.

So while the modus operandi of the high tech industry is often listen and learn, I hope that in the future we can take a little bit more time in the process of creating legislation so some of the unintended consequences can be avoided.

Thank you.

[The prepared statement of Jonathan Zuck follows:]

PREPARED STATEMENT OF JONATHAN ZUCK, PRESIDENT, ASSOCIATION FOR COMPETITIVE TECHNOLOGY

INTRODUCTION

Good afternoon, Mr. Chairman and members of the Subcommittee. I am Jonathan Zuck, President of the Association for Competitive Technology, or ACT. ACT is a national, Information Technology industry group that represents the full spectrum of tech firms, many of which are small and midsize business, that are software developers, IT trainers, technology consultants, dot-coms, integrators and hardware developers.

While ACT members vary in their businesses, they share a common desire to maintain the competitive nature of today's vibrant technology sector that has been responsible for America's "new economy."

It is my sincere honor to testify before this subcommittee today. As a professional software developer and technology educator who spent fifteen years speaking at technical conferences around the world, I am humbled by this opportunity and appreciate greatly your interest in learning more about the effects of information privacy statutes on the information technology (IT) industry. I am here to discuss the effects of the Child Online Privacy Protection Act (COPPA) and related regulations.

I think I'm the token "techie" on this panel—so I look forward to getting into some real life experiences that have arisen under COPPA. I want to begin by saying that protecting a child's privacy is of paramount importance to the IT industry and me. I do not want to suggest that there we should diminish our efforts to protect children's privacy. My testimony today is focused on the events surrounding the development of COPPA and the subsequent rulemaking as well as the impacts they, and in particular the final COPPA rulemaking, have had on small IT business. The unintended consequence of COPPA's implementation I believe is that rather than providing a marked increase in privacy protection, that the cost to comply with COPPA has led some "kid friendly" sites to have to curtail operations or shut down completely.

The Development of COPPA

As you are aware, Congress enacted COPPA in late 1998 after a recommendation by the Federal Trade Commission (FTC). It was made part of the Omnibus Consolidated and Emergency Supplemental Appropriations bill for fiscal year 1999. Notably, the legislation was passed without mark-up hearings in either the House or the Senate. In other words, there was none of the detailed deliberation or scrutiny of the legislation's language that ordinarily accompanies a bill's passage through Congress. Consequently, there is no committee report on the bill, either from the House or from the Senate. During the course of 1998, government officials and private industry representatives expressed concern about children's privacy, and their statements appear in the Congressional record. FTC Chairman Robert Pitofsky testified before the Telecommunications, Trade, and Consumer Protection Subcommittee of the House Commerce Committee on July 21, 1998, on Privacy in Cyberspace. The Center for Democracy and Technology, America Online, the American Library Association, and Chairman Pitofsky submitted testimony to the Communications Subcommittee of the Senate Commerce Committee on September 23, 1998. However, only two statements by Sen. Richard Bryan (D-Nev.) form the authoritative legislative history of the Act—one statement introducing the legislation, and another as a part of the conference report for the Omnibus bill.[1] As I will discuss further, I believe that many now realize that there are lessons to be learned from how quickly COPPA moved through the legislative process.

COPPA contains a requirement that the FTC issue and enforce rules concerning children's online privacy. The FTC issued a notice of proposed rulemaking on August 11, 1999 and received 132 comments during the 45-day comment period. During its deliberations, the FTC also held a public workshop aimed at helping the agency understand how industry might try to implement the rule. The final rule was issued on November 3, 1999 and became effective April 21, 2000.[2]

COPPA Requirements

As I mentioned before, it is the COPPA rule that has had the greatest impact on small IT companies. The COPPA rule applies to operators of commercial websites and online services directed to children under age 13, where personal information is collected. The rule also applies to operators of general interest sites with actual

[1] See 144 Cong. Rec. S8482-03 (July 17, 1998) (Statement of Sen. Bryan) and 144 Cong. Rec. S12741-04, S12787 (Oct. 21, 1998) (Statement of Sen. Bryan).

[2] 16 C.F.R. part 312.

knowledge that they are collecting information from children under 13. Those covered by the COPPA rule must (1) post a privacy policy and links to the policy; (2) give parents notice of its information practices; (3) with certain exceptions, obtain verifiable parental consent before collecting, using or disclosing personal information from children; and (4) provide parental access to information collected from children, and the opportunity to delete such c information and to opt out of future collection.

Privacy Policy and Notice—The Rule requires operators to post a policy that includes: (a) the names and contact information for all operators; (b) the types and amount of personal information collected through the site; (c) how personal information would be used; (d) whether the personal information would be disclosed to third parties, the types of business in which those third parties are engaged, whether those third parties have agreed to take steps to protect the information and a statement that parents have the right to refuse consent to the disclosure of information to third parties; (e) that the operator may not condition a child's participation in an activity on the provision of more personal information than is necessary to participate in the activity; and (f) that parents may review, amend or delete a child's personal information.[3] This policy and links must be in a place where "a typical visitor [to the site] would see the link without having to scroll down form the initial viewing screen."[4]

Verifiable Parental Consent—Operators are required to obtain verifiable parental consent *before* the use or disclosure of a child's personal information, including consent to material changes in the collection or use of the information.[5] In addition, operators must give the parent the option to consent to the collection and use of the child's information without automatically consenting to its disclosure to third parties.[6] The operator must use reasonable mechanisms to verify that the consent is actually from the child's parent.[7] These mechanisms include: (a) providing a consent form; (b) requiring a parent to use a credit card in connection with the transaction; (c) having a toll free telephone number staffed by trained personnel; (d) using a digital certificate that uses public key technology; and (e) using an e-mail accompanied by a PIN or password obtained through one of the aforementioned methods.[8] There are four exceptions to the prior consent requirement.[9] The exceptions are situations (a) where the operator collects the child's name or online contact information solely for providing notice under section 314.4 of the Rule, (b) where the operator collects online contact information solely to respond to a one time specific request from the child and is not used to recontact the child, (c) where the operator collects the online contact information to respond directly to more than one request from a child provided the information is use for no other purpose and (d) where the operator collects the name and online contact information to protect the safety of a child participant on a site or online service provided that reasonable efforts were made provide a parent notice per section 312.4(c).

Right of Parent to Review a Child's Personal Information[10]—Once a child has provided personal information, a parent may request the following: (a) a description of the specific types or categories of personal information collected by the operator (e.g., name, address, telephone number, e-mail and hobbies); (b) the opportunity at any time to refuse to allow the operator to further use or collect a child's personal information and direct the operator to delete the information and (c) a reasonable means to review any personal information gathered from the child.

The "Net" Effects of COPPA

Many commentators, while sensing the importance of protecting a child's privacy, objected to complex and burdensome nature of the COPPA Rule.[11] Indeed, some comments suggested that confusion based on the complexity of these regulations could diminish their effectiveness. Further comments noted, and I agree, that the rule as promulgated places barriers (e.g., costs) that can inhibit the growth and development of the Internet. Given this, the question that must be asked is: How effective have the COPPA rules been at protecting children's online privacy, and at what price?

---

[3] 16 CFR 312.4(b)(2).
[4] 16 CFR 312.4(b)(1).
[5] 16 CFR 312.5(a)(1) (emphasis added).
[6] 16 CFR 312.5(a)(2)
[7] 16 CFR 312.5(b)(1)
[8] 16 CFR 312.5(b)(2)
[9] 16 CFR 312.5(c).
[10] 16 CFR 312.6 et seq (emphasis added).
[11] See, e.g., comments of the American Advertising Federation and National Retail Federation,

COPPA's Effectiveness

One way to measure COPPA's effectiveness is to look at compliance. The FTC has completed random "sweeps" of web sites to check for compliance. The FTC has found that approximately half are in compliance with COPPA's requirements. Those who are not are receiving e-mails urging them to comply and that the FTC will "will monitor web sites to determine whether legal action is warranted."

The private sector is also looking at the effectiveness of COPPA compliance. A study released last month by Joseph Turow of the Annenberg School of Communication at University of Pennsylvania titled, *Privacy Policies on Children's Websites: Do They Play By the Rules?* found that of 162 top children's web sites, 114 (or 70%) linked to a privacy policy as envisioned under section 312.4 of the Rule.[12] The study noted that of the 48 sites that did not post a privacy policy, 32 (or 20%) did not collect personal information from children and only 17 sites posted no policy yet collected personal information. The study thus concluded that because 90% of sites "correctly followed COPPA in posting or not posting a link" this component of the rule is successful.[13] One success story in this vein is MaMaMedia.com which allows children to participate in "engaging activities help them gain technological fluency and expand their minds through playful learning." This site has a link to its privacy policy on its home page and on the registration page. The policy explains why it asks kids to register, what information it collects, tells parents that members can change information or cancel an account, allows members to opt out of receiving e-mail from MaMaMedia, explains its use of cookies, provides the name, phone number, postal address and e-mail address of someone to contact regarding its privacy policy, and asks parents to provide a parental e-mail address on the kids' registration page.

Despite the high level of compliance, the study points out the flaw in relying on compliance as the sole measure of effectiveness. The study found that "the biggest problem with privacy policies was the time to figure out what they said."[14] Clearly, this is an unintended consequence of the COPPA rule. However, the depth of the rule's requirements made this result inevitable. The enforcement provisions of the rule obviate the creation of a simple, clearly understandable privacy policy that may inadvertently end up costing hundreds of thousands of dollars.[15] This would lead me to question the overall effectiveness of the privacy policies and suggest that this is not a model for future legislation or regulation.

Another unintended but practical result that undermines COPPA's effectiveness is that it is aimed at children's sites that provide educational and fun experiences for children while missing adult sites that could do real harm. Steven G. Bryan, President and CEO of Zeeks.com made the following analogy in his public comments on the Rule, which I find persuasive:

> "Imagine a child walking down a street and arrives at 2 movie theaters, one across the street from the other. The one on the left side is well lit, plays only G-rated movies, is staffed by adults who monitor and supervise behavior, and serves good wholesome food in the snack bar (I consider Red Vines to be Wholesome). The theater on the right side plays R-rated movies, has little adult presence, is dark, and serves junk food. This law, if applied to my metaphorical world, would require parental permission before entering the G-Rated theater, but would require none whatsoever to enter the R-rated one. Where do you think the kids will go? We will drive children away from the very sites designed for them."

Moreover, as California Computer News noted:—While the drafters of COPPA appear to have had good intentions, it's unfortunate that their lack of foresight into the law's affects could mean an end to many of the most educational, creative and fun websites available to kids."[16]

The Costs of Compliance

While much is unknown as to what benefits will come from regulating privacy, there is already evidence of harm. The FTC concluded in its certification to avoid a Regulatory Flexibility analysis that, "any additional costs of complying with the Rule, beyond those imposed by the statute or otherwise likely to be incurred in the

---

[12] Joseph Turow, *Privacy Policies on Children's Websites: Do they Play By the Rules?* At 9.
[13] Id. at 10.
[14] Id. at 17.
[15] Web site owners that don't comply with COPPA face civil penalties of up to $11,000 per incident.
[16] Justine Kavanaugh-Brown, *New Law Sends Children's Sites Scrambling, California Computer News,* June 2000.

ordinary course of business, are expected to be comparatively minimal." [17] Were they ever wrong. Each and everyday, small IT companies make decisions critical to their survival. The complexity and costs associated with a regulatory scheme such as COPPA force these companies to forgo other needed investments or incur significant additional costs. For example, Wall Street Journal Interactive reported that FreeZone, a web portal for kids between 8 and 14, estimates it will spend about $100,000 per year to comply with COPPA. Another company that I previously mentioned, Zeeks.com, pulled all of its interactive content because the $200,000 per year cost to employ chat-room supervisors, monitor phone lines to answer parents' questions, and process COPPA permission forms was "the straw that broke the camel's back."

ZDNet News has reported that complying with COPPA could cost as much as $500,000. One of our members tells us that they spend 10% of their total resources complying with COPPA requirements. The brunt of the costs mentioned above are associated with hiring and continually training personnel to program and monitor the site as well as to answer parents' questions and requests for access. There are also direct costs, including ongoing programming and tracking to meet the notice, consent and access provisions of the Rule.It is also worth noting that not all of the COPPA requirements, as interpreted by the FTC, seem to flow directly from the legislative language. For instance, the COPPA legislation generally prohibits Web site operators and online service providers from "collecting" personally identifiable information from children without parental consent. I am not a lawyer, but to me, this general rule makes sense if you are a business and you affirmatively and actively are trying to gather information from children. To me, that is what "collecting" information means.

However, under Section 312.2 of the FTC's Rule, the act of collecting includes "**enabling** children to make personal information publicly available through a chat room, message board or other means" (except where the operator deletes any personal information before it is made public).[18] This is an extraordinarily broad definition of what it means to "collect" information. Taken to its extreme, it means that every Web site that offers a bulletin board service or a chat room is "collecting" information about its visitors (even if the site operator never stores or, let alone, looks at the information). It also means that, under the COPPA rule, all those sites arguably would have to institute blocking or monitoring and parental consent mechanisms if the operator learns that a single child has used the bulletin board service or chat room. To address this possibility, the FTC has said that "the Commission likely will not pursue an entity that is an "operator," but has not facilitated or participated in, and has no reason to know of, any Rule violation." [19] But even that statement does not alter the fact that COPPA could affect every site on the Web that offers some form of bulletin board service. This outcome is all the more troublesome when, in my mind, it is not at all clear that that is what Congress intended.

Moreover, any site that implements a parental consent mechanism must also have a means for authenticating children and their parents; otherwise, the site has no way of knowing either who a child is or who is granting consent on behalf of this child or seeking access to the child's personal information. Indeed, authentication is essential to

the COPPA compliance scheme since nothing could be more detrimental to children's' on-line privacy than allowing the wrong person to gain access to a child's data. As noted in the "Final Report of the FTC Advisory Committee on Online Access and Security," however, authentication always involves a tradeoff between security and ease of access—strong authentication often makes it burdensome and difficult to establish an account or set up a profile.[20] In complying with COPPA, therefore, sites that do not ordinarily "collect" personal information about children must also take on the additional burden and costs of implementing appropriate authentication techniques.

The Role of Technology and Consumer Empowerment

The softening economy has already caused venture capital funds to dry up and created a rash of layoffs among IT start-ups that are working hard to carve a niche in the e-commerce sector. Burdening these entrepreneurs with more laws would squeeze out many hundreds of smart people with sound business models.

---

[17] 64 Fed. Reg. 22761 (Apr. 27, 1999).
[18] 16 C.F.R. 312.2(b) (emphasis added).
[19] FTC's Statement of Basis and Purpose at fn. 55.
[20] See Final Report of the FTC Advisory Committee on Online Access and Security, May 15, 2000, Section 2.6; available online at http://www.ftc.gov/acoas/papers/finalreport.htm.

Using rich technology and empowering consumers (i.e., parents), in addition to sound public policy is perhaps the most effective way to protect a child's online privacy. There are products available to parents to assist them in protecting their child's online experience. For example, Microsoft offers "Kids Passport" which is a service that helps you conveniently protect and control your children's online privacy. You can control what information your children can share with participating Web sites, and what those sites can do with that information. In addition, you have the flexibility of making specific choices for each child and for each site, all in one convenient, centralized location.

One of the most interesting technologies coming down the pike is the platform for privacy preferences (P3P), which is an extension of some of the technology that exists today. Sponsored by the World Wide Web Consortium (W3C), P3P is a framework for products and practices that will let World Wide Web users control the amount of personal information they share with Web sites. It's described as a "privacy assistant." Using a P3P application, a parent can work with their child to enter appropriate personal information once and not have to repeatedly reenter it at different Web sites. The P3P application can inform the user of a Web site's practices with regard to gathering and reusing its visitors' personal information. Parents will thus be able to limit the information that a specific site can obtain.

There are software products on the market that allow you to generate a privacy policy that can be read by a browser as well as one which can be read by humans. It is therefore very easy to participate in the P3P movement and become a good actor on the Net. Once the standards have ironed themselves out, it will be possible for a browser to detect the privacy policy of the site you are about to visit and compare it to the preferences you have set. The browser can then warn you of a difference and help you to decide what sort of information you should and shouldn't share with the site. Sometimes, it's just this sort of friendly reminder that is all that is needed to help consumers remain conscious of this issue and protect their information accordingly.

ACT advocates a third prong to our online privacy position, which perhaps is the most important one—consumer education and empowerment. Industry must do its part to provide the necessary tools and information to consumers so they feel educated and empowered when using the Internet.

CONCLUSION—AVOID THE LAW OF UNINTENDED CONSEQUENCES

In my discussion today, we've hit upon some of the key factors that I see as a software developer and a tech futurist that determine how effective a privacy regulation like COPPA is at providing children with safe and personal Internet experiences. COPPA was the product of a rushed process and I want to commend the Chairman and this committee on taking the time to thoroughly think about and discuss the small business perspective before crafting a comprehensive privacy law. COPPA and its regulations are limited in scope yet have significant impacts on the IT industry. I urge you to keep this in mind when debating whether to enact sweeping privacy laws that will impact every industry. Industry and Congress must work together to address parental demands and weed-out the bad actors in the privacy space thereby enhancing consumer privacy, safety, and confidence.

Mr. STEARNS. I thank the gentleman.

Mr. Mierzwinski.

STATEMENT OF EDMUND MIERZWINSKI

Mr. MIERZWINSKI. Thank you, Chairman Stearns, Mr. Towns, members of the committee. My name is Ed Mierzwinski. I'm with the U.S. Public Interest Research Group which is national association of State PIRGs. Although my testimony today is only on behalf of the PIRGs, I want to point out that U.S. PIRG, along with Consumers Union are founding members of the new privacy coalition. The privacy coalition is a broad group of consumer privacy, civil liberties, family based and conservative organizations that share strong views about the right to privacy. We had previously worked together against the intrusive know your customer rules and for a number of pieces of legislation offered last year by members of the congressional privacy caucus, co-chaired by members of the Energy and Commerce Committee, Mr. Barton and Mr. Markey. And you

can look at our website of the coalition and find out the broad range of organizations in the United States that support strong privacy protections at privacypledge.org.

The emphasis of my testimony today is going to be on the relationship between the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act, two laws which consumer groups worked very hard to update the Fair Credit Reporting Act in 1996 and to ensure that in 1999, Gramm-Leach-Bliley included a privacy provision, Title V.

It's important to note that both these pieces of legislation were enacted against a backdrop of privacy nightmares. Prior to passage of the Fair Credit Reporting Act in 1970, consumers had no control over the accuracy of their credit records and other consumers who were the subjects of what are known as investigative consumer reports under the act, were the subjects of hearsay and subjective interviews with their neighbors that were often very abusive of consumers' private rights. And as a result, the Congress worked very hard and enacted the Fair Credit Reporting Act. But then the industry merged from a number of local companies into a set of national companies. As the companies merged into national data bases, the error rates skyrocketed in the 1990's and credit reporting became the No. 1 complaint to the Attorneys General and the Federal Trade Commission. The result was a coalition of consumer groups starting in 1989, worked with Members of Congress to try to strengthen the bill. We ultimately succeeded in 1996, although there were compromises made. Among those compromises was the notion added, at the insistence I should say we will not let this bill to give consumers greater rights become a law unless we are given the following exemption and the financial industry in 1996 obtained the exception from the definition of Fair Credit Reporting Act's definition of a credit report for the sharing of information among affiliates, which then became an issue in the Gramm-Leach-Bliley Act, of course.

The second problem primarily that we have had with the Fair Credit Reporting Act is the notion that it fails to encompass all information under its umbrella and the exception that FTC granted in 1993 for credit headers is our example there.

Then we move to 1999, the Gramm-Leach-Bliley Act, the privacy nightmares that were described to the Congress, first among the affiliates of the NationsBank Company, Nation Securities was shared information about CD account holders which had then tried to get buy derivatives, very sophisticated financial instruments normally purchased by people like Warren Buffet. And the second privacy nightmare that was exposed right before passage of that bill was the U.S. Bank sharing of information, confidential consumer information with the telemarketer Member Works which then billed consumers for products they hadn't ordered, because guess what, U.S. Bank gave Member Works the account number of the consumers.

Now the principal problem that consumer groups have with Gramm-Leach-Bliley is that it does not, in fact, meet all of what are known as the code of fair information practices which is a broad set of consumer rights originally drafted by HEW and that then applied to the Privacy Act of 1974 that governs information

use by the Federal Government. And our view is that notice is not enough. The bulk of the privacy protection in Gramm-Leach-Bliley is primarily notices. These notices are very long. They're very uninteresting. They're very dull, actually. They don't provide meaningful privacy protection. Ultimately, companies have the right to share information among their affiliates and with numerous third parties, even if a consumer chooses to opt-out. And consumer groups and privacy organizations believe that privacy laws should be based on all of the fair information practices, not only on the notice practice. Consumers should provide consent, meaningful consent before information is shared with either affiliates or third parties and that is the primary recommendation that we have to improve the Gramm-Leach-Bliley Act is that the loophole for information sharing, among affiliates and third parties that are providing services on behalf of the bank, be closed and that consumers always have a right to consent and that the current opt out right be changed to an opt-in right.

The testimony that I've provided to the committee goes into greater detail on all of these matters. I want to close by saying that a number of the witnesses have talked about preemption and the industry has launched a campaign around the country and herein Washington to convince Congress not to go farther and not to pass stronger privacy laws. As you know, the Gramm-Leach-Bliley Act allows the states to go further and enact stronger laws. Disappointingly, the industry is also out in the states not only trying to block passage of stronger laws, but trying to roll back existing laws and I would suggest that that is the wrong way to go and I would urge you to look closely at protecting the right of the states in any legislation that you consider to continue to pass stronger laws.

Thank you very much.

[The prepared statement of Edmund Mierzwinski follows:]

PREPARED STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, U.S. PUBLIC INTEREST RESEARCH GROUP

Chairman Stearns, Representative Towns and Members of the Committee, thank you for the opportunity to testify before you today. As you know, U.S. PIRG serves as the national lobbying office for state Public Interest Research Groups, which are independent, non-profit, non-partisan research and advocacy groups with members around the country.

U.S. PIRG is also a founding member of the Privacy Coalition, established this year by a broad range of consumer, privacy, civil liberties, family-based and conservative organizations that share strong views about the right to privacy. The groups had previously worked together on a more informal basis in opposition to the intrusive Know-Your-Customer rules and in support of financial privacy proposals offered in the 106th Congress by members of the Congressional Privacy Caucus, co-chaired by Energy and Commerce Committee members Joe Barton and Ed Markey. Groups endorsing the coalition's legislative candidate Privacy Pledge are listed at the website PrivacyPledge.Org.

The emphasis of my testimony today is on the two major laws affecting financial privacy—the 1999 Gramm-Leach-Bliley Financial Services Modernization Act [Public Law 106-102, 15 U.S.C. § 6801, et seq. enacted November 12, 1999 and its interrelationship with the 1970 Fair Credit Reporting Act [Public Law No. 91-508, 15 U.S.C. § 1681 et seq. (October 26, 1970)]. We concur with the testimony today of Consumers Union on information privacy issues more broadly.

SUMMARY

The 1970 Fair Credit Reporting Act (FCRA), its major 1996 amendments, and Title V, Privacy, of the Gramm-Leach-Bliley (GLB) Act were all enacted in response to privacy nightmares. Unfortunately, the 1996 FCRA amendments included an af-

filiate-sharing exception to the definition of credit report, allowing companies to share confidential consumer information subject to very few consumer protections. This meant the Congress had to consider privacy issues related to affiliate-sharing when it enacted GLB.

Although GLB does not go as far as consumer and privacy groups wanted, it should not be weakened. The federal financial regulatory agencies correctly interpreted statutory intent when they included Social Security Numbers in the definition of Non-Public Personal Information under the act. The lawsuit seeking to overturn the rule, filed by several firms that sell credit headers (previously unregulated locater products that include Social Security Numbers obtained from financial institution customers) should be dismissed. In addition, the federal financial regulatory agencies correctly defined the term "financial institutions" broadly to encompass all firms engaged in financial activities.

The Gramm-Leach-Bliley Act should be strengthened by extending and expanding its current opt-out choice provision. Consumers should be granted an opt-in consent right before non-public personal information is shared with either affiliates or third parties.

Providing informed consent is one of a set of Fair Information Practices that give consumers control over the use of their confidential information. Efforts by industry groups to "dumb-down" the Fair Information Practices should be resisted. Notice is not enough.

BACKGROUND

The basic structure of information privacy law is to place responsibilities on organizations that collect personal data and to give rights to individuals that give up their data. This is sensible for many reasons, including the fact that it is the entity in possession of the data that controls its subsequent use. Information privacy law also promotes transparency by making data practices more open to scrutiny and encourages the development of innovative technical approaches.[1]

Privacy laws, particularly in the United States, are widespread and have invariably come about in response to new technologies and new commercial practices. From the telephone, to the computer database, to cable television, electronic mail, videotape rentals, and the Internet, the American tradition is to establish a right of privacy in law to enable the development of new commercial services.

While it is true that the U.S. has recently relied on a sector-by-sector approach to privacy, rather than an over-arching privacy law, the convergence of industry sectors that is occurring has accelerated the need for consideration of an over-arching privacy law, which would protect consumers both online and offline in all transactions. An example of this convergence is the changes in the financial marketplace that necessitated enactment of the Gramm-Leach-Bliley Act. As privacy expert Marc Rotenberg has noted, it is now time to consider such an over-arching privacy law:

> Those who argue that the United States has typically protected privacy by self-regulation and industry codes know very little about the long tradition of privacy legislation in this country. It is, however, correct to say that the United States, over the last twenty years, has taken a sectoral approach as opposed to an omnibus approach to privacy protection in the private sector. But it is also important to note that the sectoral approach has several weaknesses. For example, we have federal privacy laws for video records but not for medical records. There are federal privacy laws for cable subscriber records but not for insurance records. I think the problems with the sectoral approach will become increasingly apparent as commerce on the Internet grows. The Internet offers the ideal environment to establish uniform standards to protect personal privacy. For the vast majority of transactions, simple, predictable uniform rules offer enormous benefits to consumers and businesses. It is also becoming increasingly clear that the large industry mergers in the telecommunications and financial services sectors have made the sectoral approach increasingly obsolete. Firms now obtain information about individuals from many different sources. There is a clear need to update and move beyond the sectoral approach.[2]

THE CODE OF FAIR INFORMATION PRACTICES

Ideally, consumer groups believe that all privacy legislation enacted by either the states or Congress should be based on Fair Information Practices, which were originally proposed by a Health, Education and Welfare (HEW) task force and then embodied into the 1974 Privacy Act. That act applies to government uses of information.[3] Consumer and privacy groups generally view the following as among the key elements of Fair Information Practices:

- limitation to collection of necessary information (purpose specificity),

- notice of the existence of all databases to data subjects who are then granted a concomitant right of disclosure of their record to review, dispute and correct errors,
- a restriction on secondary uses without consumer consent,
- a guarantee that data collectors maintain the accuracy and security of databases,
- no preemption of state or local laws affording greater protection,
- and, a private right of action for data subjects if the other rights have been violated.

Consumer groups disagree with industry organizations over whether certain self-regulatory or statutory schemes are adequately based on Fair Information Practices. Industry groups often seek to block legislation or offer substitute legislation intended to "dumb-down" the Fair Information Practices:

- First, industry groups seek to substitute a weaker opt-out choice, instead of providing opt-in consent before secondary uses,
- Second, industry groups claim that notice is enough. They claim that disclosure and correction rights are unnecessary.
- Third, they support preemption of stronger state laws and also contend that either agency enforcement or self-regulation is an adequate substitute for a consumer private right of action.

HISTORY OF CONSIDERATION OF FAIR CREDIT REPORTING ACT AND GRAMM-LEACH-BLILEY PRIVACY PROVISIONS

(1) The Need For a Fair Credit Reporting Act

U.S. PIRG has long been interested in financial information privacy issues. In 1989, we first testified before the Congress on the need for amendments to the 1970 Fair Credit Reporting Act (FCRA). At that time, in a series of hearings, Congress noted a shocking rise in the number of complaints about credit report inaccuracies to state attorneys general and the Federal Trade Commission.

The 1970 act had been enacted in response to two major problems. First, consumers had no control over the use or accuracy of their factual credit reports (called "consumer reports" in the statute). Second, job, credit and insurance applicants had been victimized by abusive collection of information, by credit bureaus, for the preparation of "investigative consumer reports." An investigative consumer report is a credit report that is based on subjective and hearsay interviews with neighbors and co-workers.[4]

In 1991, we published the first of a series of PIRG reports on the accuracy and privacy of consumer credit reports. To date, we have published six reports on credit reporting and identity theft issues. Three reports have evaluated the accuracy of credit reports:

- A PIRG report based on a Freedom of Information request to the FTC found credit reporting inaccuracies were the leading complaint to the FTC from 1991-93.
- A second key finding is that as many as one in three credit reports may contain serious errors that could cause the denial of credit, housing, insurance or even a job. This finding has been duplicated in Consumers Union studies.

Three other reports in the series have investigated the growing crime of identity theft, which affects hundreds of thousands of consumers each year. Our latest report found that victims spend two years or more removing an average of $18,000 in fraudulent charges from their credit reports. The crime is made easier by easy access to the bits and pieces of personal information that make up a consumer's financial persona. Just last month, newspaper stories reported on how sloppy financial industry security practices enabled a high-school dropout to steal the identities of numerous celebrities:

> Using computers in a local library, a Brooklyn busboy pulled off the largest identity-theft in Internet history, victimizing more than 200 of the "Richest People in America" listed in Forbes magazine, authorities say. Abraham Abdallah, 32, a pudgy, convicted swindler and high-school dropout, is suspected of stealing millions of dollars as he cunningly used the Web to invade the personal financial lives of celebrities, billionaires and corporate executives, law enforcement sources told The Post.[5]

U.S. PIRG's reports on identity theft and the hassles victims are put through by financial firms include a detailed legislative platform of reforms needed to prevent identity theft and improve the accuracy of credit reports[6]. Among the key reforms we have identified would be legislation to close the so-called credit header loophole[7], which has been partially closed by the Gramm-Leach-Bliley financial privacy rule approved by the 7 federal financial agencies. We discuss the controversial credit header loophole below.

(2) The Need For Title V (Privacy) In Gramm-Leach-Bliley

The Gramm-Leach-Bliley Financial Services Modernization Act was enacted to respond to changes in the marketplace. Banks, insurance companies and securities firms were more and more selling products that looked alike. The firms wanted the privilege of and synergies derived from selling them all under one roof. Yet, the Gramm-Leach-Bliley Act was also enacted against a backdrop of financial privacy invasions, and members wanted to ensure that the new law wouldn't make things worse. Consumer and privacy groups argued that if the Congress was going to create one-stop financial supermarkets, then privacy protections ought to extend to all information sharing, whether with affiliates or with third parties. At the time, two examples were given of the need for stronger privacy laws.

One of these examples involved an affiliate-sharing arrangement:

The Nationsbank/NationsSecurities case resulted in a total of $7 million in civil penalties. Nationsbank shared detailed customer information about maturing CD holders with a securities subsidiary, which then switched the conservative investors into risky derivative funds.[8]

The second example involved a bank sharing confidential customer information with a third party telemarketer:

In June 1999 the Attorney General of Minnesota sued US Bank for sharing confidential customer "experience and transaction" information with third-party firms for telemarketing and other purposes. The telemarketer doing business with US Bank, Memberworks,[9] had contracts with numerous other banks, as did at least one other competitor, BrandDirect,[10] which has also been the subject of consumer complaints. In the U.S. Bank litigation, it was determined that not only was U.S. Bank sharing detailed customer dossiers with the telemarketer, it was also sharing account numbers. This allegedly allowed Memberworks to use deceptive telephone scripts to convince consumers to take trial offers. The consumers didn't think they had ordered any goods, but since the bank had shared their account numbers, it turns out that they had. U.S. Bank, in 1999, signed a multi-million dollar settlement with the state of Minnesota.

In addition to providing for an nonaffiliated third-party opt-out, Gramm-Leach-Bliley included a specific provision purporting to prevent future U.S. Bank debacles. The new law prohibits sharing account numbers for marketing purposes. Unfortunately, the agencies have interpreted that law to allow sharing of "encrypted" account numbers, if there is no way for the telemarketer to "un-encrypt" the number. In our opinion, this protection is a "virtual," or meaningless, protection, since a telemarketer could "push a button on a computer" connected to the bank and authorize the billing of a consumer who didn't actually order anything.

In December 2000, the Minnesota Attorney General filed yet another suit, this one against Fleet Mortgage, an affiliate of FleetBoston, for substantially the same types of violations as U.S. Bank engaged in. While some consumers may presume that their credit card company, as a matter of routine, is going to attempt to pitch junky, over-priced and tawdry products such as credit life insurance, credit card protection and roadside assistance, the practice is now spreading to mortgage affiliates as well. The state's complaint succinctly explains the problem that occurs when your trusted financial institution shares confidential account information with third party telemarketers. The complaint states that when companies obtain a credit card number in advance, consumers lose control over the deal:

> Other than a cash purchase, providing a signed instrument or a credit card account number is a readily recognizable means for a consumer to signal assent to a telemarketing deal. Pre-acquired account telemarketing removes these short-hand methods for the consumer to control when he or she has agreed to a purchase. The telemarketer with a pre-acquired account turns this process on its head. Fleet not only provides its telemarketing partners with the ability to charge the Fleet customer's mortgage account, but Fleet allows the telemarketing partner to decide whether the consumer actually consented. For many consumers, withholding their credit card account number or signature from the telemarketer is their ultimate defense against unwanted charges from telemarketing calls. Fleet's sales practices remove this defense.[11]

This complaint alleges that the company was providing account numbers to the telemarketer. In our view, Gramm-Leach-Bliley needs to be amended so that telemarketers cannot initiate the billing of a consumer who has not affirmatively provided his or her credit card or other account number. Whether this case stems from pre-Gramm-Leach-Bliley acquisition of full account numbers, or post-Gramm-Leach-Bliley encrypted numbers or authorization codes, is not the question. In either case, consumers have lost control over their accounts.

DO EITHER THE FCRA OR GLB MEET FAIR INFORMATION PRACTICES TESTS?

Although U.S. PIRG generally believes that consumer rights in credit reporting need to be strengthened to prevent errors and to prevent privacy invasions, the FCRA is largely based on Fair Information Practices. Companies cannot access credit reports without a permissible purpose (providing both for security and a limited form of consent), consumers have strong dispute and correction rights, and consumers have a modest private right of action. Where the FCRA largely falls short is where it interfaces with the Gramm-Leach-Bliley Act, the subject of the hearing today[12]:

1) First, the 1996 FCRA amendments exempted the sharing of "experience and transaction" information between affiliates from the definition of credit report. Under the Gramm-Leach-Bliley Act, information shared between and among affiliates (and even some third parties) for secondary purposes is not subject to either an opt-in or an opt-out. The act does provide that when financial institutions obtain so-called "other" information, that consumers must be granted a right to opt-out of sharing, even among affiliates. This right must be disclosed on GLB privacy policies.

2) Second, the 1996 amendments failed to close the so-called "credit header" loophole, established by the FTC in a 1993 consent decree with TRW (now Experian). The credit header loophole allowed credit bureaus to separate a consumer's so-called header or identifying information—including his name, address, Social Security Number and date of birth—from the remainder of his credit report and sell it outside of the FCRA's consumer protections. In March 2000, the FTC held that dates of birth are used to calculate credit scores and are therefore credit-related information. It removed them from headers. The final Gramm-Leach-Bliley financial privacy rules issued later that spring by the 7 federal financial agencies defined Social Security Numbers as non-public personal information. Although the issue is currently in litigation, the agencies are, in our view, correctly interpreting the law to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out.

The Gramm-Leach-Bliley Act falls short of meeting Fair Information Practices in several areas as well.

- First, it fails to require any form of consent (either opt-in or opt-out) for most forms of information sharing for secondary purposes, including experience and transaction information shared between and among either affiliates or affiliated third parties.
- Second, while consumers generally have access to and dispute rights over their account statements, they have no knowledge of, let alone rights to review or dispute, the development of detailed profiles on them by financial institutions.
- The act does provide for disclosure of privacy policies, although a review of a sample of privacy policies suggests that companies are not following the spirit of GLB. None are fully explaining all their uses of information, including the development of consumer profiles for marketing purposes. None are listing all the types of affiliates that they might share information with. None are describing the specific products, most of which are of minimal or even negative value to consumers, that third party telemarketers might offer for sale to consumers who fail to opt-out. Yet all the privacy policies make a point of describing how consumers who elect to opt-out will give up "beneficial" opportunities.

THE AFFILIATE SHARING LOOPHOLE IN THE FCRA AND GLB

In 1996, when the Congress finally enacted comprehensive amendments to the FCRA, a fundamental dispute between consumer groups and the Federal Trade Commission, on one side, and the financial industry, on the other, concerned whether or not confidential consumer information shared between and among financial affiliates would be subject to the FCRA's consumer protection provisions. In 1996, the Congress chose to grant an exception to the definition of consumer report, for transaction and experience information shared between and among "companies affiliated by common control." The Congress also allowed companies to share information obtained from third parties (third parties such as the consumer herself, her credit report, and her job references) but granted the data subject a right to opt-out of the sharing of this information, even among affiliates. This right must be disclosed on GLB privacy policies.

Consumer groups contend that as financial firms get larger and contain more subsidiaries and affiliates, they may no longer need to contact credit bureaus for their own underwriting and marketing decisions. Consumers will not be able to shop around for credit (let alone for privacy policies). Gramm-Leach-Bliley can only be expected to expand the capabilities of financial services holding companies to make credit decisions without using credit bureaus. Consumers will then face credit deni-

als, or increases in the cost of credit, without benefit of the full panoply of FCRA rights.

Basically, if affiliate A directly obtains a credit report and denies you a loan, you have full FCRA rights. If you fail to opt-out of "other" information sharing, and your credit report and application information are retained by the bank, affiliate B could make credit decisions without contacting a credit bureau. A consumer does not then have FCRA rights. If these practices grow, and if more financial institutions begin to make decisions based on their own internal profiles, or even establish internal subsidiary credit bureaus exempt from the FCRA's coverage, the effects not only on privacy, but also on competition and credit allocation, will be significant. Some consumers will not even be told they have been denied credit.

Consumer groups and other privacy proponents generally contend that information should not be shared for secondary purposes without the subject's affirmative (opt-in) consent and that this protection should apply to both affiliate and outside (third-party) transactions. During consideration of the bill that became GLB, HR 10, the full Commerce Committee, in its wisdom, chose to support by acclimation, a bipartisan financial privacy amendment supported by privacy groups offered by Reps. Markey and Barton. The compromise amendment would have granted consumers an "opt-out" right whether confidential information was shared between affiliates or with third parties. The Markey-Barton amendment would have given consumers the right to an opt-out that would have protected all their financial information from being used for secondary purposes by either an affiliate or any third party. As Representative Barton stated on the floor during consideration of HR 10:

> The question I ask this body and this country is: If we are concerned about the selling and sharing of information to third parties, should we not be just as concerned about the selling, sharing, transmitting, or accessing that information inside of these affiliates if there are going to be dozens or hundreds of these affiliates? ...Until we solve the riddle of handling information within the affiliate structure, we do not have privacy. We do not have privacy.[13]

Unfortunately, neither the Banking Committee, nor the House leadership, nor the Senate, agreed. The Commerce Committee privacy amendment was not passed in the Banking Committee and was not even considered on the floor of either House, even though it passed the full Commerce Committee.

The final version of Gramm-Leach-Bliley defines non-public personal information that is to be protected under the act. It then bifurcates third party companies into two groups. The first, affiliated third parties, are treated as affiliates for information-sharing purposes. Companies can share experience and transaction information (including non-public personal information) between and among both affiliates and affiliated third parties, which may be providing services on behalf of the bank, regardless of a consumer's opt-out preference. However, after the effective date (1 July 2001) of GLB, such information can only be shared with nonaffiliated third parties if the consumer has been granted notice and been given an opportunity to opt-out. There are two primary implications of this limited protection. First, consumers will have the ability to limit access by third party telemarketers to their confidential financial information. Second, they may be able to protect their Social Security Numbers from secondary use by information brokers.

THE LAWSUITS OVER THE NARROWING OF THE CREDIT HEADER LOOPHOLE

Consumer and privacy groups strongly contend that easy access to consumer identifying information leads to stalking and identity theft. Even if it did not, groups strongly support restrictions on the secondary use of Social Security Numbers, which were never intended as a national identifying number yet form the key for establishing someone's location or identity. In other areas, such as Drivers' License privacy, the Congress has sought to narrow the availability of Social Security Numbers.[14] In the 106th Congress, Social Security Number protection legislation named for Amy Boyer, the first-known victim of an Internet stalker, was defeated after it was seen that the proposal actually was a Trojan Horse that expanded the availability of Social Security Numbers, primarily to customers of the Individual References Services Group. IRSG member companies include credit bureaus and other information firms engaged in the sale of non-public personal information to locater services, debt collectors, information brokers, private detectives and others.[15]

In 1993, the Federal Trade Commission granted an exemption to the definition of credit report when it modified a consent decree with TRW (now Experian). The FTC said that certain information would not be regulated under the Fair Credit Reporting Act. The so-called credit header loophole allowed credit bureaus to separate a consumer's so-called "header" or identifying information from the balance of an otherwise strictly regulated credit report and sell it to anyone for any purpose.[16] The

FTC's theory was that credit headers included information that ostensibly did not bear on creditworthiness and therefore was not part of the information collected or sold as a consumer credit report. The sale of credit headers involves stripping a consumer's name, address, Social Security Number and date of birth from the remainder of his credit report and selling it outside of the FCRA's consumer protections. Although the information, marketing and locater industries contend that header information is derived from numerous other sources, in reality, the primary source of the most accurate and best credit header data is likely information provided by financial institutions with monthly credit updates.

In March 2000, the FTC held that dates of birth are credit-related information and removed them from headers.[17] The final Gramm-Leach-Bliley financial privacy rules issued later that spring by the 7 federal financial agencies defined Social Security Numbers as non-public personal information. Although the issue is currently in litigation, the agencies are, in our view, correctly interpreting the law. Since Social Security Numbers are held to be non-public personal information, the rule acts to prevent the sharing of Social Security Numbers unless consumers are given notice of the practice and a right to opt-out. As the FTC explains in the preamble to its Gramm-Leach-Bliley Financial Privacy Rule:

> The Commission recognizes that § 313.15(a)(5) permits the continuation of the traditional consumer reporting business, whereby financial institutions report information about their consumers to the consumer reporting agencies and the consumer reporting agencies, in turn, disclose that information in the form of consumer reports to those who have a permissible purpose to obtain them. Despite a contrary position expressed by some commenters, this exception does not allow consumer reporting agencies to re-disclose the nonpublic personal information it receives from financial institutions other than in the form of a consumer report. Therefore, the exception does not operate to allow the disclosure of credit header information to individual reference services, direct marketers, or any other party that does not have a permissible purpose to obtain that information as part of a consumer report. Disclosure by a consumer reporting agency of the nonpublic personal information it receives from a financial institution pursuant to the exception, other than in the form of a consumer report, is governed by the limitations on reuse and redisclosure in § 313.11, discussed above in "Limits on reuse." **Those limitations do not permit consumer reporting agencies to disclose credit header information that they received from financial institutions to nonaffiliated third parties**...If consumer reporting agencies receive credit header information from financial institutions outside of an exception, the limitations on reuse and redisclosure may allow them to continue to sell that information. This could occur if the originating financial institutions disclose in their privacy policies that they share consumers' nonpublic personal information with consumer reporting agencies, and provide consumers with the opportunity to opt out.[Emphasis added, Footnotes omitted][18]

In their lawsuits filed to block the inclusion of Social Security Numbers in the Gramm-Leach-Bliley definition of non-public personal information, the credit bureaus and other IRSG members the firms make any number of kitchen-sink arguments against the rule.[19] Among the most important are their claims that the Gramm-Leach-Bliley Act does not affect the FCRA, that the breadth of the agencies' rules goes beyond statutory intent, and that the agencies should not be granted any deference under the Supreme Court's Chevron[20] test.

First, the firms argue that Gramm-Leach-Bliley includes a savings clause (Section 6806) that the law does not "modify, limit, or supersede the operation of the Fair Credit Reporting Act." This view is without merit, since no part of the Fair Credit Reporting Act allows the sale of credit headers. As the FTC points out in its preamble to the rule, "To the extent credit header information is not a consumer report, it is not regulated by the FCRA and a prohibition on its disclosure by a consumer reporting agency consistent with the statutory scheme of the G-L-B Act in no way modifies, limits or supercedes the operation of the FCRA.[21]"

Second, the firms argue that the agencies went too far in defining non-public personal information and that the rule should be rejected on these grounds. They further argue that the agencies are not entitled to deference in their statutory interpretations under the Chevron test[22]. The consumer groups strongly disagree with the firms on these counts. First, it was very clear from the legislative history of GLB that the Congress intended confidential information provided to financial institutions as a condition of obtaining an account should be construed as non-public personal information. Second, seven separate federal financial agencies, all with expertise in financial industry matters, concurred on identical regulations.

Based on the record, then, if anything, the seven agencies that issued an identical joint rule agencies should be granted sweeping Chevron deference "ultra." The seven

agencies have done an admirable job of determining that GLB requires the deletion of Social Security Numbers from credit headers, unless consumers are given notice and an opportunity to opt-out. When credit bureaus sell credit reports, they are entitled to the FCRA savings clause of GLB. When credit bureaus sell credit headers, they are clearly nonaffiliated third parties selling non-public personal information. Disappointingly, rather than comply with Congressional intent, the firms have chosen to roll the dice in the courts.

ASSAULT ON STATE LAWS AND THE SO-CALLED "COSTS" OF PRIVACY

The 1996 amendments to the Fair Credit Reporting Act partially preempt the right of the states to enact stronger laws, especially in the area of prohibiting affiliate sharing, until 2004. Although Gramm-Leach-Bliley, overall, is sweepingly preemptive, Title V includes a state law savings clause, the so-called Sarbanes amendment that allows states to enact stronger privacy laws (Section 6807). We disagree with industry groups that this provision's applicability to affiliate sharing is trumped by Title V's FCRA savings clause. Unfortunately, the financial industry has not only sent lobbyists out en masse to oppose enactment of stronger state financial privacy laws under consideration in numerous states, it has also sent them out to attack existing laws. This week, North Dakota apparently was convinced to gut an existing financial privacy law and Vermont is under extreme pressure to do so as well. We urge the states to reject the financial industry's unfounded and blackmail-like claims that they stop selling products in your state unless you accede to their wishes and eviscerate your consumer laws.

The financial services and other information industries have also unleashed a massive public relations assault purporting that privacy costs too much money and, incredibly, according to some news stories, may bring down the economy. U.S. PIRG intends to review the industry-funded studies that form the alleged basis for these claims in greater detail. We urge the committee to evaluate the claims made in these industry-funded studies in great detail before acting on them, if at all. The American people have demonstrated strong support for strong privacy protections. In our view, the costs of not protecting privacy—increased identity theft and stalking, sale of unsatisfactory telemarketed products, loss of the right to be left alone—easily outweigh these purported costs to industry. We will provide the committee with more analysis as it becomes available.

CONCLUSION

We appreciate the opportunity to testify before you on the important matter of financial privacy. Although neither the Fair Credit Reporting Act nor the Gramm-Leach-Bliley Act go as far necessary to protect consumer privacy, the laws together play an important role in establishing a minimal framework of financial privacy protection. We look forward to working with the committee to strengthen the laws.

Footnotes

[1] See the "Privacy Law Sourcebook, 2000: United States Law, International Law and Recent Developments," by Marc Rotenberg, Electronic Privacy Information Center, for a comparision of all important privacy laws.

[2] Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center and Adjunct Professor, Georgetown University Law Center, on The European Union Data Directive and Privacy Before the Committee on International Relations, U.S. House of Representatives May 7, 1998 <http://www.epic.org/privacy/intl/rotenberg-eu-testimony-598.html>

[3] As originally outlined by a Health, Education and Welfare (HEW) task force in 1973, then codified in U.S. statutory law in the 1974 Privacy Act and articulated internationally in the 1980 Organization of Economic Cooperation and Development (OECD) Guidelines, information use should be subject to Fair Information Practices. Noted privacy expert Beth Givens of the Privacy Rights Clearinghouse has compiled an excellent review of the development of FIPs, "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy." October 1997. <http://www.privacyrights.org/AR/fairinfo.html> The document cites the version of FIPs in the original HEW guidelines, as well as other versions: Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973 [From The Law of Privacy in a Nutshell by Robert Ellis Smith, Privacy Journal, 1993, pp. 50-51.]

1. Collection limitation. There must be no personal data record keeping systems whose very existence is secret.

2. Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

[4] Consumer groups oppose legislation, HR 3408, introduced in the 106th Congress (and expected to be re-introduced) by Rep. Pete Sessions to exempt workplace misconduct reports from the FCRA. We recognize that an unintended consequence of the 1996 amendments to the FCRA unwisely gives investigatory subjects a warning that they are under investigation. The solution is not to exempt workplace investigations, a major area of abuse of workers, from the FCRA. See 4 May 00 testimony of the National Consumer Law Center and U.S. PIRG, with an appendix provided by the AFL-CIO, that details the problem: <http://www.house.gov/financialservices/5400sau.htm>

[5] See New York Post, 20 March 2001, "HOW NYPD CRACKED THE ULTIMATE CYBER FRAUD" <http://dailynews.yahoo.com/htx/nypost/20010319/lo/how__nypd__cracked__the__ultimate__cyberfraud__1.html>

[6] See "Nowhere To Turn: A Survey Of Identity Theft Victims," May 2000, CALPIRG, U.S. PIRG and the Privacy Rights Clearinghouse, for the latest version of the platform: <http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>

[7] In the 106th Congress, bi-partisan legislation approved by the Ways and Means Committee (HR 4857, Shaw-Matsui-Kleckza) would have eliminated Social Security Numbers from credit headers. Several other bills would close the credit header loophole.

[8] See SEC Release No. 7532 And Release No. 39947, May 4, 1998, Administrative Proceeding Against NationsBank, NA And NationsSecurities, File No. 3-9596, In The Matter Of : Order Instituting Cease-And-Desist Proceedings Pursuant To Section 8a Of The Securities Act Of 1933 And Sections:15(B)(4) And 21c Of The Securities Exchange Act Of 1934 And Findings And Order Of The Commission. See <http://www.sec.gov/enforce/adminact/337532.txt> (Note, total civil penalties of nearly $7 million includes fines paid to other state and federal agencies, as well as to the SEC.) From the order:"NationsBank assisted registered representatives in the sale of the Term Trusts by giving the representatives maturing CD lists. This provided the registered representatives with lists of likely prospective clients. Registered representatives also received other NationsBank customer information, such as financial statements and account balances. These NationsBank customers, many of whom had never invested in anything other than CDs, were often not informed by their NationsSecurities registered representatives of the risks of the Term Trusts that were being recommended to them. Some of the investors were told that the Term Trusts were as safe as CDs but better because they paid more. Registered representatives also received incentives for their sale of the Term Trusts."

[9] On Friday, 16 July 1999, the Minnesota Attorney General filed suit against Memberworks. At least four other states (Florida, California, Washington and Illinois) are investigating the firm. See The Washington Post,. "Telemarketer Deals Challenged in Suit, Sale of Consumer Financial Data Assailed," by Robert O'Harrow Jr, Saturday, July 17, 1999; Page E01.

[10] For articles on BrandDirect and Chase Manhattan, see for example, The Seattle Post-Intelligencer, "You may be a loser—buying something you didn't want", by Jane Hadley, Thursday, April 8, 1999 or Newsday, "Company Had Her Number/Woman discovers to her surprise card issuer gave out account data" by Henry Gilgoff, 9 May 1999.

[11] 28 December 2000, Complaint of State of Minnesota vs. Fleet Mortgage, see <http://www.ag.state.mn.us/consumer/news/pr/Comp—Fleet—122800.html>

[12] FCRA also preempts state laws in most respects, until 2004, and fails to provide free access to credit reports except in limited circumstances. We oppose these two provisions.

[13] Floor debate on HR 10, Congressional Record, Page H5513, 1 July 1999.

[14] See enacted 2000 amendments to the Drivers Privacy Protection Act by Senator Shelby. For more information about privacy invasions caused by access to Social Security Numbers, see the new book, "War Stories III," by Robert Ellis Smith, Publisher, Privacy Journal, <http://www.privacyjournal.net>

[15] See the U.S. PIRG Fact Sheet, "Why The Amy Boyer Law Is A Trojan Horse" at <http://www.pirg.org/consumer/trojanhorseboyer.pdf>

[16] The industry has since established an association, the Individual References Services Group, which purports to manage a voluntary self-regulation that regulates sale of non-public personal information included in credit headers to what it terms "authorized commercial and professional users." In our view, information brokers can easily slip through IRSG's net.

[17] See Trans Union Order, March 2000.

[18] Excerpted from pages 80-83, Federal Trade Commission, 16 CFR Part 313, Privacy Of Consumer Financial Information, Final Rule <http://www.ftc.gov/os/2000/05/glb000512.pdf>

[19] Several lawsuits have been filed, including by Trans Union, Individual References Services Group, and other credit bureaus. Although cross-motions for summary judgments have been filed by both sides in the U.S. District Court for the District of Columbia, no oral argument has been scheduled.

[20] Chevron USA vs. Natural Resources Defense Council, 467 US 837 (1984).

[21] Pages 81, Federal Trade Commission, 16 CFR Part 313, Privacy Of Consumer Financial Information, Final Rule <http://www.ftc.gov/os/2000/05/glb000512.pdf>

[22] See Pages 14-18, Memorandum in Support of Trans Union LLC's Motion For Summary Judgment, Trans Union vs. Federal Trade Commission, Civil Action No 1:00 CV 02087 (ESH), 1 Nov 00.

Mr. STEARNS. I thank the gentleman.

Let me start the round of questioning with Mr. Plesser. Some people have advocated an opt-in regime for future privacy protec-

tion. In COPPA, the law doesn't require an opt-in for use of further information. Am I correct in that?

Mr. PLESSER. Well, it does have verifiable consent of a parent for the collection of use. There are four exemptions to it, so it owes its opt-in/opt-out terminology gets a little vague, but it does have a pretty strong consent basis for it. So it could be called opt-in and then it has some exceptions to opt-out.

Mr. STEARNS. The question could it be considered opt-in or opt-out, yes or not? Can it be considered opt-in or opt-out?

Mr. PLESSER. I would primarily call it an opt-in legislation.

Mr. STEARNS. Okay. So you have to consent to go in. If we adopt some type of opt-in regime for general privacy protection, it may seem unusual if we provided a weaker standard for children than non-children. I mean we're trying to get some consistency, whether opt-in or opt-out. Do you have a way that you look at this that you could tell us that this opt-in would be for this kind of policy and this opt-out would be for this type of policy?

Mr. PLESSER. Well, I think there's room for both. I do think as was discussed before that it varies on the type of information. I think for medical information, some detailed financial information, information collected from kids, a consent or opt-in is appropriate. I think for general information, marketing information, material generally collected from websites, I think an opt-out is sufficient and I think one has to examine the information.

Mr. PLESSER. Mr. Torres, I'd ask this question and you were probably here when I talked to Panel 1 about the Gramm-Leach-Bliley bill. And you have criticized in your opening statement the current privacy statute, HIPAA, COPPA, Gramm-Leach-Bliley. Do you believe that we should revisit every one of these and redesign them or is it that you think it's okay the way it is and perhaps is it politically possible to do it?

Mr. TORRES. Mr. Chairman, if I could be clear, I think that Consumers Union believes that the privacy provisions in Gramm-Leach-Bliley Act are completely inadequate and should be revisited.

Mr. STEARNS. Completely inadequate and should be revisited.

Mr. TORRES. And should be revisited. With respect to the medical privacy provisions of HIPAA, while we think there are some shortcomings that need to be addressed, we don't agree that the rule should be gutted and we don't believe that the rule shouldn't be implemented.

With respect to COPPA, I think for the most part the intent of that legislation was right on target, the fact that parents should have some control over the information collection, information collected from their children when they go on line. Is it appropriate to address some of the problems with it? Probably so. Do we need to roll the protections back? No.

Mr. STEARNS. In the Gramm-Leach-Bliley, I guess you heard there's going to be almost 21 notices in a year given to all the people. Don't you think that's sufficient?

Mr. TORRES. It was interesting. I spoke not to long after that law was passed to a group of members of the insurance industry and they started blasting me for getting such a bad law passed.

Mr. STEARNS. yeah.

Mr. TORRES. I said actually I'm not the one who drafted that. The consumer groups aren't the ones that put that together. It was something agreed to by the financial services industry and put in the bill. What we simply wanted was and when you think about it what's so troublesome about telling consumers about your information collection practices? Now I've taken a look at some of the notices. I haven't seen notices from everyone and I think you'll probably see the full gamut of notices, but some of them spend five pages telling you what a great job they're doing about, you know, they care about your privacy and they will take great steps to protect it, but at the end of the day what consumers end up with under Gramm-Leach-Bliley is virtually nothing. The reason why companies can say well, we'll not even share information with third parties, is because those financial institutions don't want to deal with third parties. What would be interesting is to ask a financial institution what information they currently do or would want to do would be prohibited under the exceptions of Gramm-Leach-Bliley. That's how big the exception is.

Mr. STEARNS. Okay. Mr. Varn, as I understand it, you were a prior elected official, a State Representative or State Senator?

Mr. VARN. Both.

Mr. STEARNS. So you understand the whole process here. I thought it was interesting your comment that a set of visceral reaction that occurs and prompts legislative action. I mean only a person who had been elected can understand that. And that reaction precedes any understanding of the benefit of the use of the record so that not true balancing was used.

Let me just go to your—you tried to definitize this when you talked about the four issues of privacy: security, integrity, accuracy and privacy. What you say are distinct issues in your mind, yet last time all of us discussed them as one and the confusion results. You might just want to elaborate for the record the significance of such resultant confusion.

Mr. VARN. Oftentimes people will call something a privacy problem when it's, in fact, a security problem. People will say, for example, people's credit cards have been revealed from a website being hacked and they'll call it an invasion of privacy. Well, yes, that is, but the problem, the core problem in that case was a lack of proper security——

Mr. STEARNS. In the first place.

Mr. VARN. In the first place. The lack of investment by our Nation in security infrastructure. You started with the FBI in trying to expand a web across our country to enforce, to help our security people deal with this problem. But confusion between those two, for example, other people will say my records aren't accurate or I can't get access to them and I have a privacy concern about that. Well, that's more easily addressed by going right after the accuracy and access issue. So my point is these particular areas have more specific solutions that can address them better when we aim right. So if it's an accuracy problem, especially when public records are at stake and someone says that's not me, I didn't do that. You can go after that problem not calling it a privacy issue or restricting the record, go right after fixing the record.

The last part of this is also enforcement. Besides just breaking these up into security and integrity—and integrity is the one that's ignored. Losing your records is pretty serious and we'd have underinvested in that. But enforcement underlies all these things. We pass these laws, I've been part of that and we don't pass the regimen. We don't pass the funding. We don't put in place the methodology to actually enforce them and they end up being a hollow promise, so I'd say those are your five areas to focus on, trying to keep them distinct and aim your solutions better.

Mr. STEARNS. Just one last question for Mr. Zuck. I understand some companies have opted not to market to children under 13 years of age because of restrictions contained in the Child On-Line Privacy Protection Act. Is there a right balance or how do we find the right balance between quality, privacy protection and unbearable commercial limitations. Is there such a thing?

Mr. ZUCK. Mr. Chairman, that's a really good question. Finding that balance is the real challenge and I think part of it is by engaging in a much more open process than creating legislation in the first place. I think some of the deficiencies associated with COPPA are a function of the lack of vetting and mark-up processes that normally goes into bills and it kind of went through as a omnibus budget bill and so a lot of where the forethinking about where some of the costs that outweigh some the benefits might have arisen might have come to the surface with a better process being in place.

Mr. STEARNS. My time has expired. Mr. Towns?

Mr. TOWNS. Mr. Chairman, let me start right on that point because I think there's a piece that you sort of left out there and I don't want you to indict the Congress without us being guilty. I mean I want to make certain that what happened there is that I would point out as a matter of clarification that before passing the House and Senate as part of the appropriations bill, both the Child On-line Protection Act and the Children's On-line Privacy Protection Act were passed by both the committee and the full House under suspension of the rules. In both cases, the legislation was passed by voice vote. So I take exception to your characterization regarding that particular matter, and of course, to say to you that the fact that it passed by a voice vote I think points out that we took it very seriously and we did know what we were doing in that particular instance because it went through that process.

Mr. ZUCK. I mean obviously I wasn't trying to indict Congress, and as a programmer, I'm sure that I'm misspeaking as I speak about these processes. But I think that while the law passed one kind of language, for example, collection of data, on-line was a part of the language of the law and it was handed over to the FTC for rulemaking and that collection of data was extended to include data that wasn't, in fact, being collected by the companies, but instead, things like chat rooms, etcetera, where people were sharing data with each other and that's one of the biggest sources of costs has arisen. So I guess my point was simply that in a process of mark-ups, etcetera, that I've gotten used to seeing is that some of those things may have come to the forefront and been left less to the discretion of the FTC.

Mr. TOWNS. We do enough bad stuff so when I get a chance to defend the Congress, I want to do so, you know? That's what we're talking about here.

Mr. ZUCK. Yes sir.

Mr. TOWNS. Thank you. Mr. Torres, I left the room for a moment, I don't know whether this was dealt with or not. The University of Pennsylvania study concerned the Children's On-Line Privacy Protection Act, seems to say the law is being under-enforced and not complied with. Is that because—I think it was Mr. Zuck who said the law is flawed and not able to be complied with.

Mr. TORRES. I'm not sure if the Annenberg Study draws that particular conclusion, but what it does say is that they question whether or not some of the companies who are targeting their sites to children actually ever fully expect parents to be able to read these privacy policies that they put out. They're either too vague or not complex enough. They did cite to some sites that seemed to get that right balance where they're actually understandable. In fact, what the Annenberg Study found was that they had college educated researchers taking a look at this and it took them a little bit of time to understand what the privacy policies were all about. Why couldn't it be simple and if we want to educate parents, let's not do away with the law and say let's educate parents. Why not educate parents about what to look at on these website policies to enhance their ability to make the decisions when they go on line. That would be the thing to do, not to say oh, it's too complicated, we can't comply or we've got to draft our privacy notices in such a complex or vague way that parents don't know what's going on.

Mr. TOWNS. Mr. Plesser?

Mr. PLESSER. Yes, I would just like to comment quickly on the Annenberg Study. I think it is is the glass half full or half empty? It showed that there were 17 sites that didn't have notices on them, kids' notices, but we looked at a fair number of those 17 sites where we looked at them and I think there's legitimate argument that some of those sites were not directed at children. And I think there may be a disagreement and lawyers can disagree, people can disagree, but I think it's a pretty good argument. And I think most of what else they said was that they were concerned with graphics, with presentation. They saw one site, MaMaMedia that they thought was great and they graded other sites in kind of comparison to this, what they thought was the best.

I don't think the implication and the way I read it, was some of the sites whose graphics weren't as good or color contrast was good were illegal, it was just simply they could do better. I think that's not the same thing as saying that those sites were bad. I think its actually compliance looked pretty good and of course, the FTC and the Attorney Generals now have full authority to enforce those statutes, so Congress did provide enforcement and teeth behind that statute.

Mr. TOWNS. Mr. Zuck?

Mr. ZUCK. I think Mr. Torres brought up a point that actually underscores the irony of the situation to some extent when he said that some of these privacy policies don't appear to be written for parents. In a competitive marketplace in which children's sites are trying to compete for the confidence of parents, they're going to be

really aiming the language to be simple, to be easy to read, to interpret. In a regulatory environment, these policies are actually aimed to be read by lawyers, because those are the people that are now the ones that these sites feel they answer to rather than the parents. And I think that is part of the irony of having such a restrictive environment is that these privacy policies are written for lawyers, instead of for parents.

Mr. TOWNS. My time has expired, but let me say Mr. Mierzwinski, what are those industry groups who have challenged the FTC's rule believe they need access to a person's Social Security number and mother's maiden name?

Mr. MIERZWINSKI. Well, I think that the FTC in 1993 said that the Fair Credit Reporting Act definition of credit report did not include information in your header, that is, information about your demographics, including your name, address, Social Security number, date of birth and sometimes mother's maiden name. The FTC, consumer groups and privacy groups believe, made a big mistake when it did that. However, the Gramm-Leach-Bliley Act has classified Social Security numbers as non-public, personal information and the FTC is interpreting that to mean that if a consumer opt-out of information sharing with a non-affiliated third party, he or she deserves the right to have their Social Security number protected. So ultimately, I think that's one of the most important predictions in the limited number of protections other than notice that Gramm-Leach-Bliley provides. The companies believe that the Social Security number, I don't speak for them, but I think they believe that in addition to believing that Congress overstepped or—excuse me, that the agencies and the Congress overstepped their authority in interpreting Social Security numbers to be nonpublic personal information, the companies believe that the Social Security number is the key to your identity and that it is the key to your location in the computerized world and they want the Social Security number to establish your credit header more accurately. Consumer and privacy groups believe that consumers shouldn't have their Social Security number used for secondary purposes like this without our consent. In the Drivers Privacy Protection Act amendments that Mr. Shelby supported and passed last year, we, in fact, get greater protection of Social Security numbers in other circumstances whereas the information sales industry wants the right to sell Social Security numbers and we simply disagree with them over that.

Mr. TOWNS. Thank you for your generosity. Thank you, Mr. Chairman.

Mr. STEARNS. Sure. Mr. Terry?

Mr. TERRY. Thank you, Mr. Chairman. Mr. Mierzwinski, sorry about mispronouncing your name. Let me ask you a few questions. First of all, you mentioned a couple Omaha folks. I represent Omaha, Nebraska. By the way, Warren Buffet's real name is Warren Buffet of Omaha, if you read the article, so please note that for the record.

You also mentioned another corporate citizen that's been in the news lately, Member Works. So I want to talk a little bit about some of the accusations you've laid on the table during your testimony. They had some difficulties with the Attorney General in

Minnesota and some other states. That's duly noted, but I want to kind of work through where you think the problems are and if you are just acting on misinformation or you have facts that I don't have.

First of all, you said U.S. Bank gave the telemarketers account information. Now as I understand when we looked into this in our office, what they gave the telemarketers were name, address, phone number, but the telemarketer, the 20-year-old college student who is making the phone call, didn't have access to that person's credit card number. That part was encrypted. Is that your understanding? Because you criticized U.S. Bank for transferring to these telemarketers account information or credit card information.

Mr. MIERZWINSKI. I think that the privacy invasion and I base all of my testimony on the complaints and the settlement agreements that have been filed by the Attorney General of Minnesota in those cases. When I say that the credit card numbers or checking account numbers or in the new lawsuit recently filed by the Attorney General of Minnesota against Fleet Mortgage or the mortgage number of banks' customers were provided to the telemarketing company. Whether or not the individual telemarketer sitting at the computer kiosk who is making the call to the consumer has the credit card is not the privacy invasion.

Mr. TERRY. That's what I wanted——

Mr. MIERZWINSKI. The company has it and we still contend that that's an invasion. And I understand in some of the circumstances it was not encrypted, but may have been unencrypted.

Under Gramm-Leach-Bliley, they're still allowing, they the regulators, are still allowing the transfer of encrypted credit card numbers and other account numbers to telemarketers which we believe still allows telemarketers to deceive consumers into buying products they did not think they had bought and I excerpt from the recent Fleet Mortgage case that explains that.

Mr. TERRY. So just in this process, whether the information is encrypted and not readable to the telemarketer, it's still an invasion of privacy?

Mr. MIERZWINSKI. In our view, it is, because as the Attorney General articulates in his complaint in Fleet Mortgage, the consumer loses control over the transaction when he or she essentially is trapped into making a trial offer purchase without ever having provided his or her credit card number.

Mr. TERRY. Giving biographical data to the telemarketer is or is not an invasion of privacy according to your feelings?

Mr. MIERZWINSKI. Well, in addition, I think consumer groups believe that nonpublic personal information, in general, ought not to be provided to third parties, however, we find it especially a problem when the credit card number is either encrypted or not are provided to telemarketers in such a way that manipulative telemarketing scripts can be used to deceive consumers.

The Fleet Mortgage case, the Attorney General says according to interviews done with the telemarketing representatives themselves, they believe that up to 20 percent of their complaints are about these telemarketing products.

Mr. TERRY. I'm still trying to work through any sharing of information, just name, address and phone numbers is an invasion.

Would it still be an invasion of privacy if U.S. hired these telemarketers in-house and they were paid by U.S. Bank or is the invasion of privacy in your mind that it was transferred to an affiliate or a company unrelated to U.S. West or the fact that they're even selling something, is that what you're——

Mr. MIERZWINSKI. Well, I think you raise a very good point, Congressman, and that point is, is there a difference between sharing of information with affiliates or with third parties. And actually, consumer groups don't think that there is. Unfortunately, the Gramm-Leach-Bliley bill only provides for a consumer to have any right of even weak consent when the information is shared with third parties, that is, not affiliated third parties. You have no right to say no to the sharing of experience and transaction information with affiliates. We obviously, that's what we support as a solution as to close that loophole.

Mr. TERRY. All right, well, I appreciate that and for the record, as I understand the transaction from the telemarketers, regardless of what most of us think of telemarketing, in the process, as I understand with Member Works and Fleet, I don't know about Fleet or whatever you're talking about there, but they asked several times if they understand it's going to be billed to their credit card. And if they're being asked that succinctly, I'm having difficulty understanding the invasion of privacy.

Mr. MIERZWINSKI. Again, Congressman, according to—I've spoken with the Attorney General's staff and I've read their complaints. I've actually listened to the tapes that were provided as exhibits in the lawsuits and prior to at least in the Member Works case, prior to their settlement with the Attorney General, the Attorney General alleged, contended, whichever, that the scripts were extremely misleading and deceptive.

Mr. TERRY. Have you listened to the tapes?

Mr. MIERZWINSKI. I have copies of the tapes, yes.

Mr. TERRY. You didn't answer whether you listened to them.

Mr. MIERZWINSKI. Yes, I listened to them, yes, I'm sorry.

Mr. TERRY. My time is up.

Mr. STEARNS. The gentleman's time has expired. I would want to thank the second panel.

Mr. Varn, I had talked to Vice President Cheney about a Chief Information Officer for the U.S. Government. He's looking at that.

When did the State of Iowa institute or initiate a Chief Information Officer?

Mr. VARN. It began as a division of our General Services about three and a half years ago. It became a Department a year ago May. It's only the 28th State to have one.

Mr. STEARNS. The United Kingdom has it on the Secretary level, an e-commerce type of person.

Mr. VARN. Right.

Mr. STEARNS. I want to thank the second panel. I want to thank the members. I think this has been a balanced hearing. It's been very informative on the issues and I think we've seen that privacy is a very complex issue. Thank you, and the committee is adjourned.

[Whereupon, at 4:29 p.m., the committee was adjourned.]